GLASSWALL

An introduction to Glasswall's zero-trust CDR

Detection-based security methods play catch-up with new threats. It's time for proactive defense. 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.

With Glasswall CDR, only safe, clean and fully functioning files enter and leave an organization, allowing users to access files with full confidence

Glasswall's range of solutions satisfies varying business requirements. Our platform's highly scalable Kubernetes-based architecture allows for ultimate flexibility when deploying Glasswall CDR in your organization.

How Glasswall CDR instantly removes risk

Glasswall CDR uses our 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

Glasswall zero-trust CDR integrates anywhere documents are in motion or at rest

Cross Domain Solutions (CDS)

Supercharge Cross Domain Solutions with CDR technology that removes the reliance on detection and data wrapping. Glasswall CDR enables government departments and commercial 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.

File upload portals

Ingesting files from external parties and networks is a critical requirement for many organizations and government departments. However, there are weaknesses in current practices that can be exploited by the uploading of malicious content.

The Glasswall Embedded Engine's zero-trust sanitization capabilities can be established at various integration points within an organization's security architecture.

Cloud migration

All organizations rely on the transfer of files across trust boundaries, both within their organization, or to/from public networks, and it is critical to ensure that malicious content or risky files are not transferred during cloud migrations. Glasswall CDR provides organizations and departments with REST endpoints and a UI that harnesses the power of the Kubernetes-based Glasswall CDR Platform to process large storage containers at massive scale.

Isolated networks

Glasswall CDR provides zero-trust file protection that maintains air-gapped network isolation. Detection based solutions require an open channel to ingest updates compromising the isolation of secure networks. Glasswall's zero-trust philosophy doesn't rely on updates to protect against both zero-day and known file-based threats – ensuring maximum isolation for secure networks.

Industry critical compliance

In addition to helping companies adhere to industry guidelines and government Initiative, our CDR technology boasts patented and industry-leading features, such as Word Search and Redact, Metadata Removal and Image Analyzer. These features have been developed to help organizations to comply with other legislation, such as GDPR and the California Privacy Rights Act.