GLASSWALL

Case Study

Removing Malicious Content From Terabytes Of Critical Data

The Challenge

Glasswall was approached by a large government agency with a problem: they had terabytes of important data on an isolated network which they believed could contain unknown malicious content. They urgently required access to this data, but the only option available at the time was to 'sheep dip' it in anti-virus. Understanding that AV only offers limited protection and can leave you exposed to file-based threats for up to 30+ days, they needed a different approach that didn't rely on legacy detection-based methodologies. They were looking for a solution that would ensure that all this critical data would be safe, secure and accessible.

HM Government

On the recommendation of a leading UK intelligence agency, they turned to Glasswall to clean the data using its industry-leading Content Disarm and Reconstruction (CDR) platform.

The Technology

Unlike reactive security methods such as AV or sandboxing which attempt to identify and block malicious content, Glasswall CDR technology instantly cleans and rebuilds files to match its known good manufacturers specification – automatically removing potential threats.

This proactive approach instantly makes files and documents safe from threats, ensuring prevention against future unknown attacks, eliminating risk without compromising productivity, whilst giving users the freedom to safely access files.

Inspect

files digital DNA

Clean

risky content (by policy)

Rebuild

to known good standard

Deliver

safe, visually identical file

The Solution

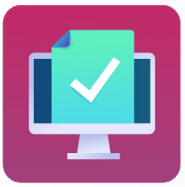
Glasswall was able to provide the government agency with a comprehensive bulk processing solution within ten days of their initial request, which has now been fully deployed.

The solution started with the deployment of the Glasswall SDK with a Command Line Interface tool (CLI) which immediately allowed the client to start cleansing the most important, urgent files. At the same time, Glasswall also presented a solution for processing files at scale, deploying two instances of the Glasswall SDK orchestrated with a Kubernetes workflow cluster, a highly scalable and compliant infrastructure. This handled the transfer of files from the untrusted location, load balancing between the two instances, and placed the clean files into a safe location. A clear audit trail of all file processing was provided, highlighting the risk mitigated in each file.

Glasswall had also provided the client with the Glasswall Desktop App, reconfigured to run on the Ubuntu OS, enabling the government agency to continue processing smaller amounts of data in a more efficient way. The entire package included ten days of comprehensive professional services to help the agency with the implementation.

Glasswall SDK

Kubernetes Workflow Cluster



Glasswall Desktop App

Bulk File Processing

The Outcome

Glasswall was able to move fast, working seamlessly with the government agency. Terabytes of data were imported into the new environment within days, providing the government agency with complete confidence they now had no malicious content.