GLASSWALL

Glasswall API

Glasswall has developed an API-first architecture in delivering our Kubernetes-based Content Disarm & Reconstruction (CDR) Platform. A typical business document file can be analyzed and protected in less than a second. That's blistering speed when you consider how long file sandboxing and AV detection can take. Furthermore, Glasswall CDR can provide on average, an 18 day protection advantage compared to other malware solutions which fail to detect zero-day threats.

Glasswall Clean Room is an application that uses Glasswall API to present file analysis and file rebuild requests to the Glasswall CDR Platform.

Key benefits

- ✓ Synchronous Cloud API endpoints to provide real-time responses to analysis and file rebuild requests, making integrations as simple as possible for developers to experience them straight away
- ✓ Asynchronous Cloud API endpoints to enable a requester to send many requests to the service and where the response can be deferred
- ✓ Dynamic content management policy for Microsoft Office and PDF files - enabling different protection options for different user audiences
- ✓ Single API request can be issued to receive both a file analysis report and to obtain a protected file, free from any malware threats
- ✓ File-detection service which accurately reports the true file format, ensuring unwanted file types are not allowed to move into the target environment
- ✓ Stand alone machine instances can act together in concert with a load-balancer to allow auto-scaling and self-healing, characterised as a disposable Kubernetes cluster configuration
- ✓ Single compute instance with 16 (virtual) cores could potentially provide CDR protection to around 40 GBs of data or approximately 57,000* files in a 24-hour period using Glasswall's CDR platform
- ✓ Flexible architecture which makes processing times a function of how much compute resource is added to the deployment environment
- ✓ Deployment via a Public Cloud, Private Cloud or On Premise

*Average file size 0.65MB

Key features

- Content management policy for Microsoft Office and PDF files which can be controlled dynamically via the API
- Two sets of REST-based API endpoints, synchronous Cloud API and Asynchronous modes to help developers devise the most effective integration approach to meet their needs
- Kubernetes-based architecture which can be deployed via a managed Kubernetes service such as AKS, EKS, GKE or OKE for Azure, AWS, Google Cloud and Oracle or as a stand alone machine instance such as an AMI (in AWS)
- Terraform deployment scripts and helm charts to support a managed Kubernetes service
- Always-on service via a range of deployment options to provide organizations with ability to establish resilient patterns, spanning multiple availability zones and regions around the world
- Cloud APIs are compliance with the OpenAPI v3.x specifications, allowing development teams to rapidly create client software integrations using codegen tools
- Deep file inspection, beyond artefacts such as the so-called magic number, to accurately report what file data suggests about the true file type

Use cases

Integration of CDR protection into a software process

File Upload / Download actions

Cross Domain Service integration

Glasswall Clean Room deployment

Integration with Proxy-ICAP service to remove threats from files transmitted across a network