



Glasswall Desktop App

Users receive files on their work computers in a variety of ways. Automatically remove potential threats from files (including threats AV software hasn't detected yet).

With Glasswall Desktop, employees can drag and drop files from the outside world into the Glasswall CDR Platform – so they're free to use files without risk.



Key benefits

- ✓ Enable users to work risk-free with any file received outside your organization
- ✓ Instantly disarm threats in files from unknown sources (e.g. a customer's USB drive)
- ✓ Users get immediate feedback on risks identified in a file and how they were removed
- ✓ Both original and the rebuilt files are retained for audit purposes



Key features

- Simply drag and drop files from local hard disk, server share, media device or cloud folder onto Glasswall Desktop App to instantly disarm malicious files
- Create safe, compliant files that are standardized to known good manufacturer's specification
- Accessible to all users – no training or special knowledge needed
- Supports the most common operating systems including Windows, MAC and Linux
- Easy, user-friendly UI
- Access Glasswall CDR engine offline through Docker container

Use cases



File uploads or downloads
from unknown source



Malware risk removal



Zero Day threat defence

How it works

The Glasswall Desktop App uses the patented Glasswall CDR Platform to inspect, clean and rebuild every file to its known good state in real-time—proactively protecting your organization against the most persistent and complex file-based threats.

