



USE CASE

Secure Email

Protect your organisation from the most stubbornly popular attack vector. With Glasswall CDR (Content Disarm and Reconstruction), users receive secure emails at the speed of business.

Remove risk in real-time

Email continues to be an effective channel for attackers seeking to breach an organisation. Anti-virus solutions can't detect new viruses as quickly as businesses need them to. [STAT] Sandboxing and detonation chambers offer a bit more protection, but slow your users down. It's time for a better way. Keep business moving with

Glasswall CDR, so employees receive safe emails without delay. It inspects, cleans and rebuilds email file attachments to their known good state in real-time—proactively protecting your organisation against the most complex and persistent threats. Glasswall removes risk in an instant (users won't even notice it's there).

Key benefits



Proactively remove threats from every email without delay or waiting for a 'Patient Zero' (i.e. how AV identifies threats)



Every email attachment that comes through – even fake emails from the CEO – is cleaned and rebuilt so it's completely secure



Analyse and disable links within the body of an email by policy to limit the risk of phishing email attacks

Key features

- Hosted on Microsoft Azure with no additional on-premises resources required
- Seamless integration with all major platforms, including O365, Microsoft Exchange and G-Suite
- Gain visibility on inbound file types and features
- Keep the formats and features you need with configurable policy for active content and file types
- Easily manage risk for your organisation with a secure web portal and flexible policy management
- Supports all key business file formats, including Binary Office, XML Office, PDF, PNG, JPEG and GIF files. (Unsupported file types are controlled by policy)
- Sub-second file processing – files are regenerated in milliseconds
- All data is encrypted and you have complete control of data retention period for up to 90 days

How it works

Glasswall CDR technology instantly cleans and rebuilds files to match their known good manufacturer's specification – automatically removing potential threats. This simple approach ensures every file in your organization is safe, without sacrificing productivity.



Inspect

files digital DNA



Clean

risky content (by policy)



Rebuild

to known good standard



Deliver

safe, visually identical file