Glasswall Proxy Solution

For SharePoint

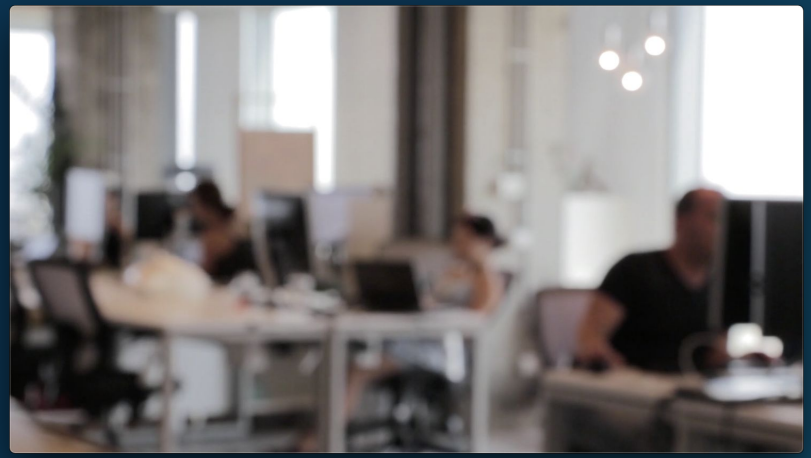
Sep 2020

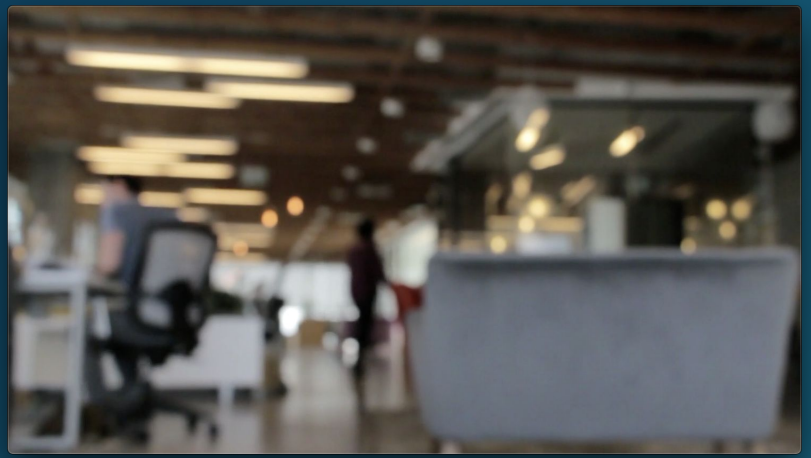
GLASSWALL

IN EARLY 2020

Users are working in a secure building

In an internal network using an internal email system and file storage solution





GLASSWALL

IN EARLY 2020

Then Covid-19 lockdown happened

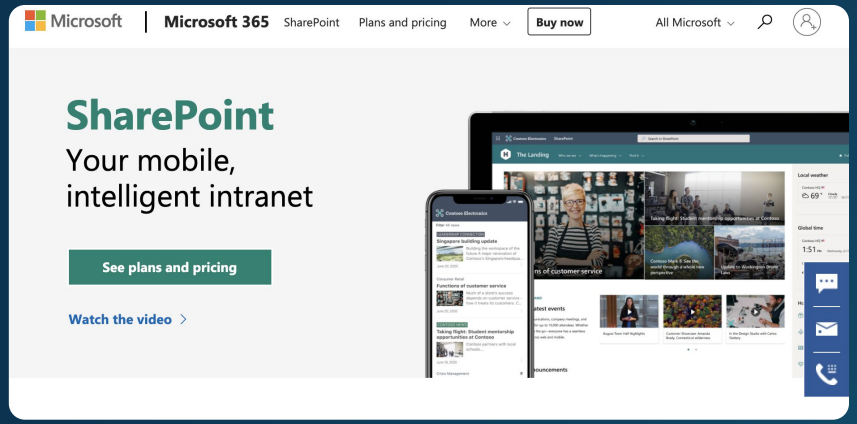
All users had to work from home

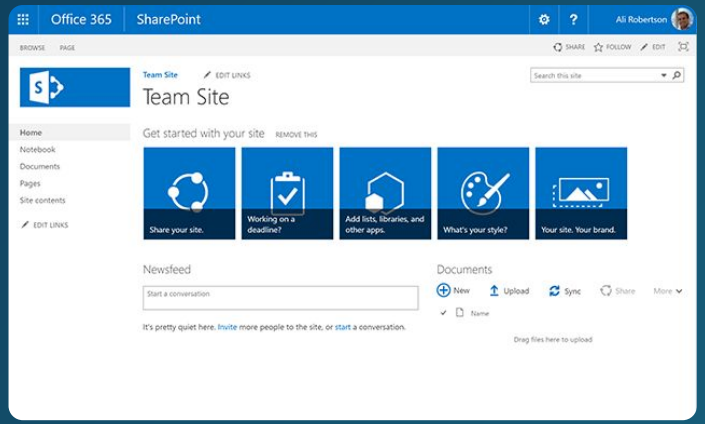
GLASSWALL

IN EARLY 2020

A short term measure was implemented to allow users to be productive from home using SharePoint

SharePoint is Part of Office 365 and is Microsoft's most popular cloud based email and file management solution



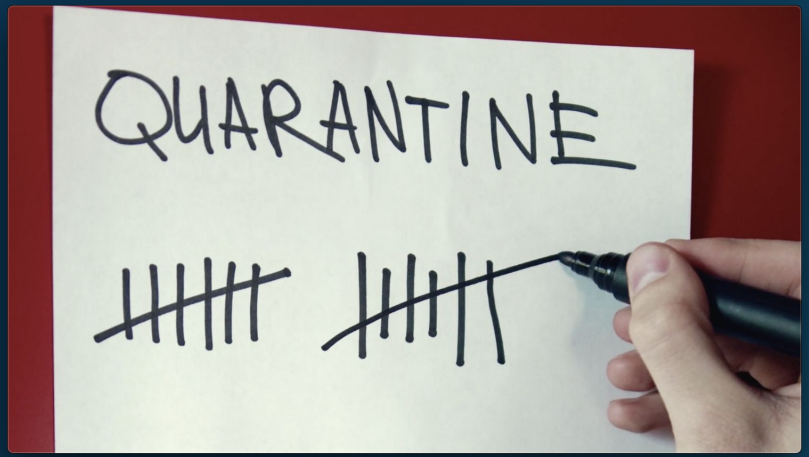


GLASSWALL

LATE 2020

Covid-19 is now under control , and users are coming back to the office

Together with new files that have been created in SharePoint

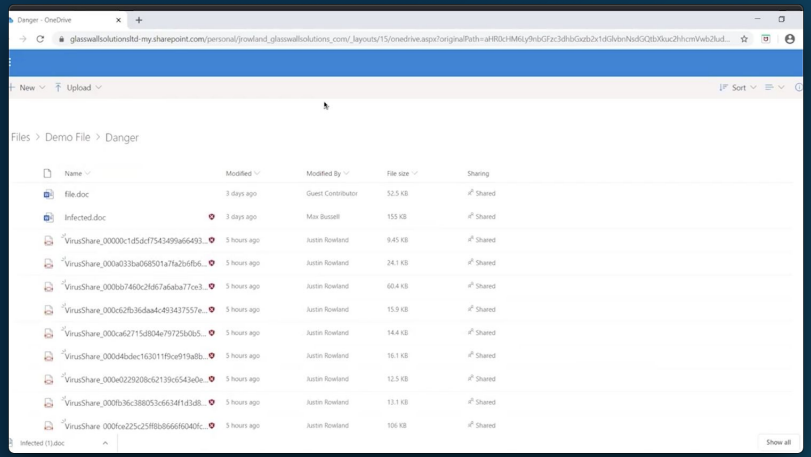


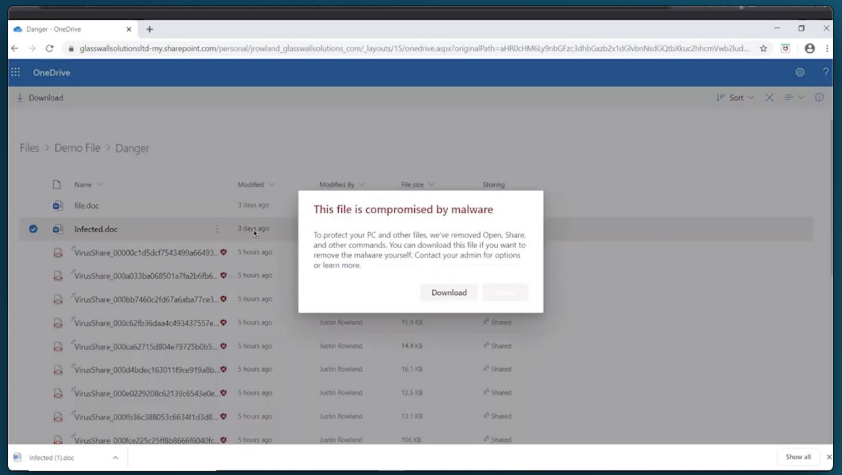
GLASSWALL

LATE 2020

Those files need to be brought into the safe network

The problem is that a number of those files might be malicious, whose payload will only trigger in internal system

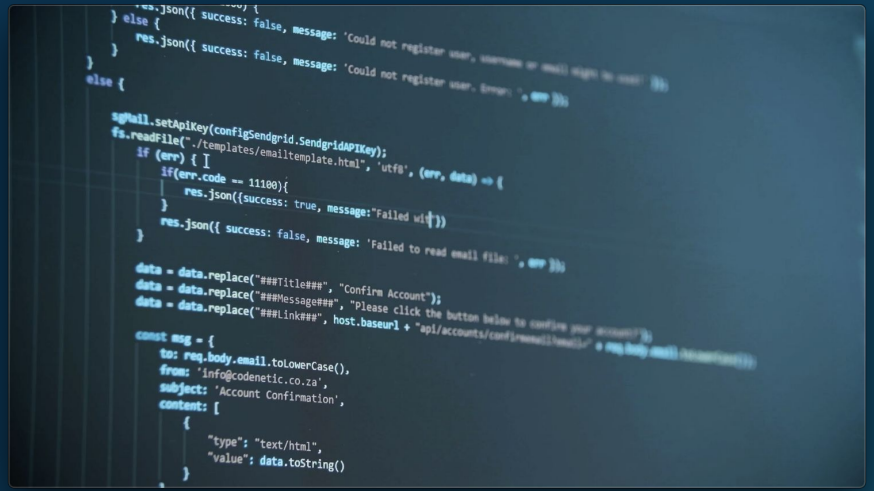


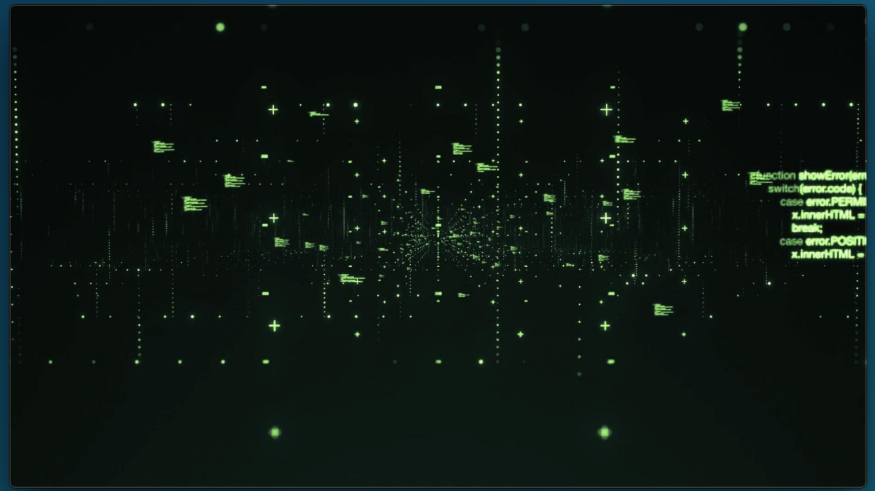


GLASSWALL

LATE 2020

What we need is a solution to safely import those files into the internal network



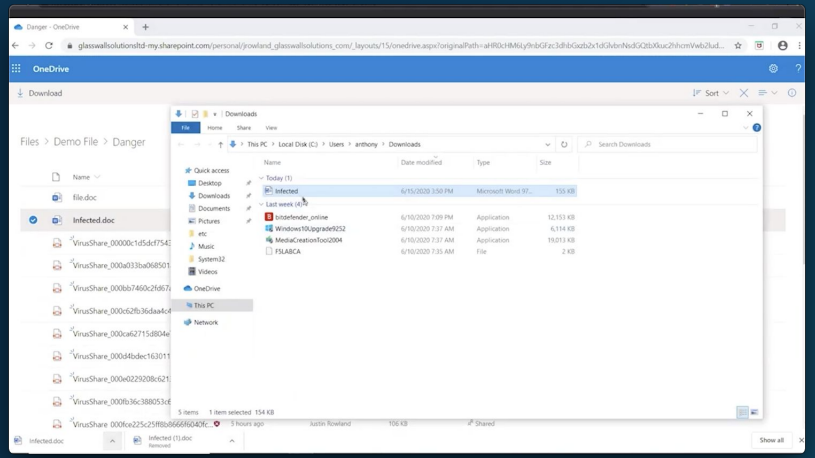


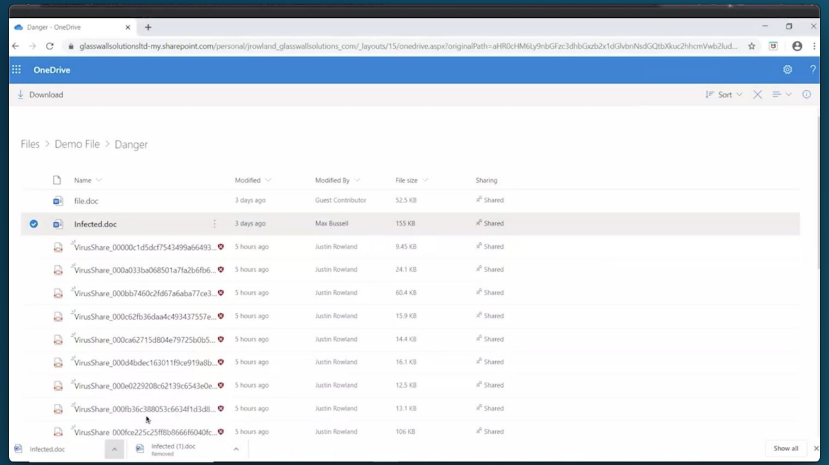
GLASSWALL

LATE 2020

Given the large number of files, this needs to happen in a transparent and user friendly way

That will limit overhead to existing IT and security teams





GLASSWALL

The solution that meets the requirement is based on 3 technological components

1

Proxy with ICAP Protocol

2

AntiVirus

3

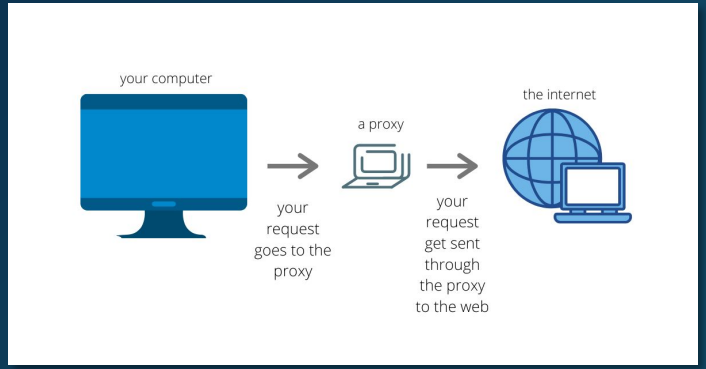
Glasswall Proxy Server

GLASSWALL

1

Proxy with ICAP Protocol

Intercepts the files between sharepoint and users who are now using the internal network



CITRIX · Symantec · netskope · zscaler · A10 · f5 · Check Point SOFTWARE TECHNOLOGIES LTD. · McAfee · SANGFOR · clearswift A HelpSystems Company

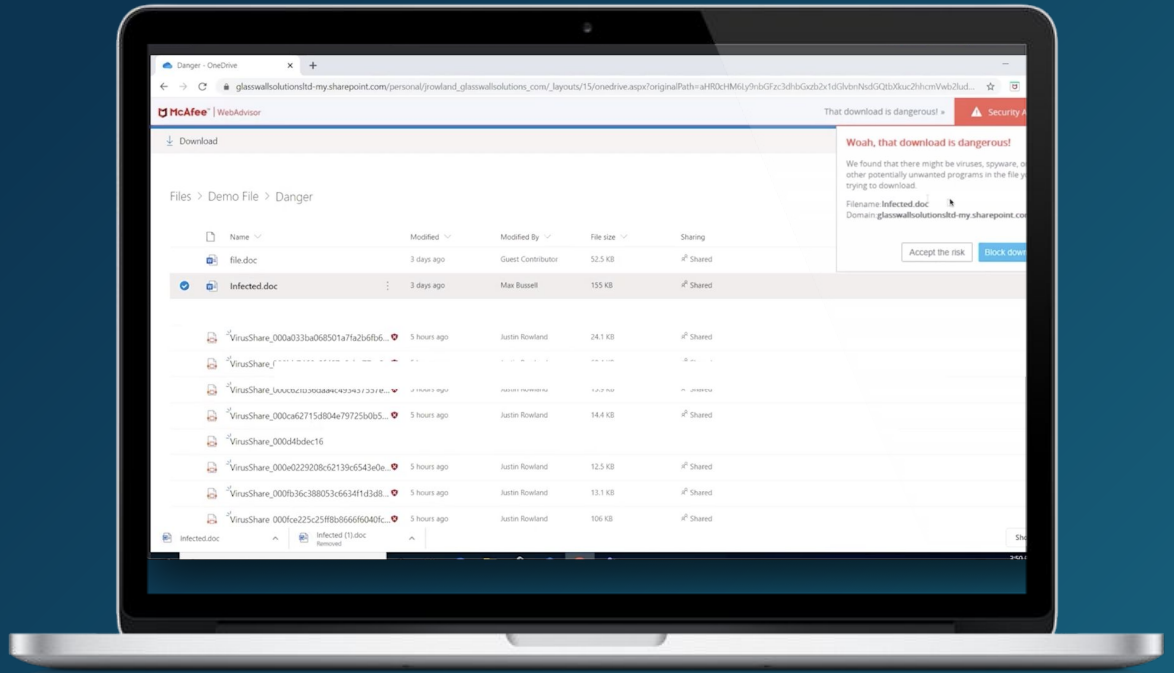
ContentKeeper · CISCO · TREND MICRO · Menlo Security · websense ESSENTIAL INFORMATION PROTECTION · iboss · FORCEPOINT · Barracuda · COMODO Certification Authority · ARRISON TECHNOLOGY · WatchGuard

GLASSWALL

2

AntiVirus

Check for known bad files

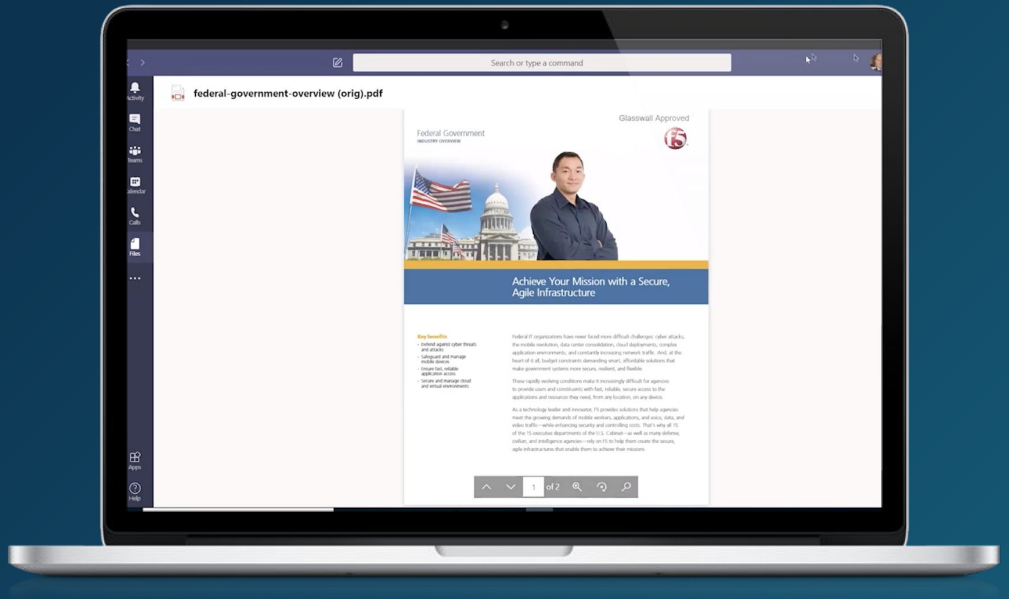


GLASSWALL

3

Glasswall
Proxy Server

Uses CDR (Content Disarm and Reconstruction) Technology to rebuild files into a ‘known good and safe’ state



Supported File Types

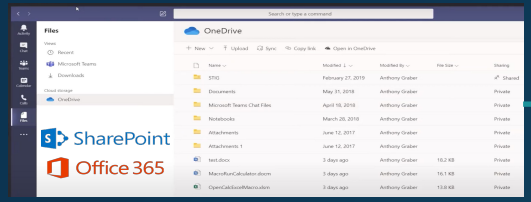
GLASSWALL

File Types	File Description
PDF	*Adobe Portable Document*
JPG GIF PNG EMF WMF TIFF GeoTIFF BMP	*Images*
DOC DOT	*MS Word 97-2003*
XLS XLT	*MS Excel 97-2003*
PPT POT	*MS PowerPoint 97-2003*
DOCX DOCM DOTX DOTM	*MS Word 2003 & later*
XLSX XLAM XLSM XLTX XLTM	*MS Excel 2003 & later*
XPPTX POTX POTM PPTM PPSX PPAM PPSM	*MS PowerPoint 2003 & later*
WAV MP3	*Audio*
MPG MP4	*Video*
PE DLL MUI EXE MACH-O COFF ELF	*Portable executables*

Rebuilding into known good

GLASSWALL

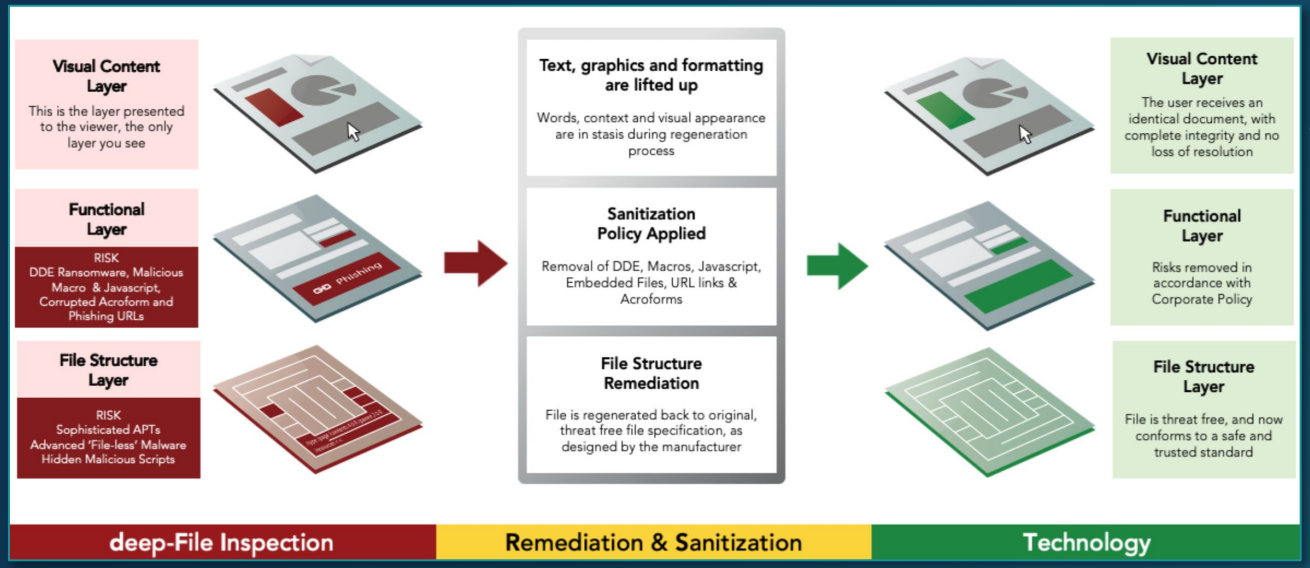
1. Files in storage could be malicious



2. Instead of looking for bad

3. Rebuild file into a known good state

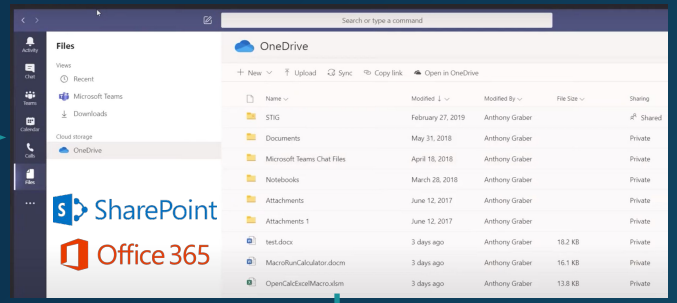
4. Glasswall creates a NEW visually identical and safe file



Solution workflow

GLASSWALL

1. User clicks on files stored on SharePoint



2. During download a Proxy (like F5) intercepts files

3. and sends them to malware detectors and Glasswall

Anti-virus

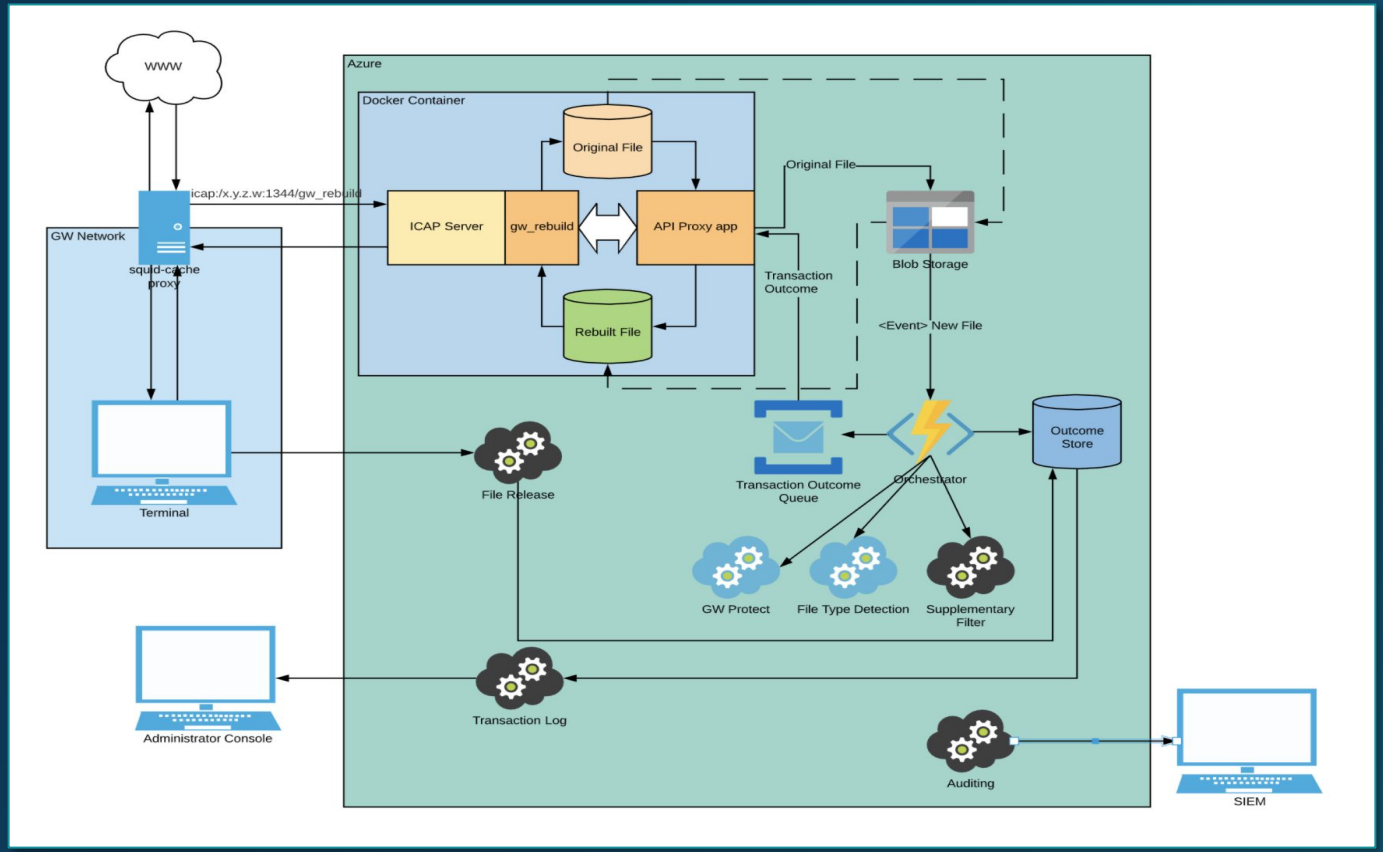
CDR

GLASSWALL

4. Glasswall creates a NEW visually identical and safe file

Cloud based Architecture (Azure)

GLASSWALL



GLASSWALL

All this will happen efficiently for a Sharepoint site that has:

- ✔ 2 Million Users
- ✔ 500 thousand active users
- ✔ Max 80 thousand concurrent file downloads
- ✔ 8 millions files
- ✔ 80 Terabytes of data

  (1 Terabyte = 1024 Gigabytes)

GLASSWALL

PROXY SERVER

SHAREPOINT CASE STUDY

https://www.youtube.com/watch?v=IhWnyV53j8o

GLASSWALL

Thanks