

Glasswall Proxy Solution

For SharePoint
Sep 2020



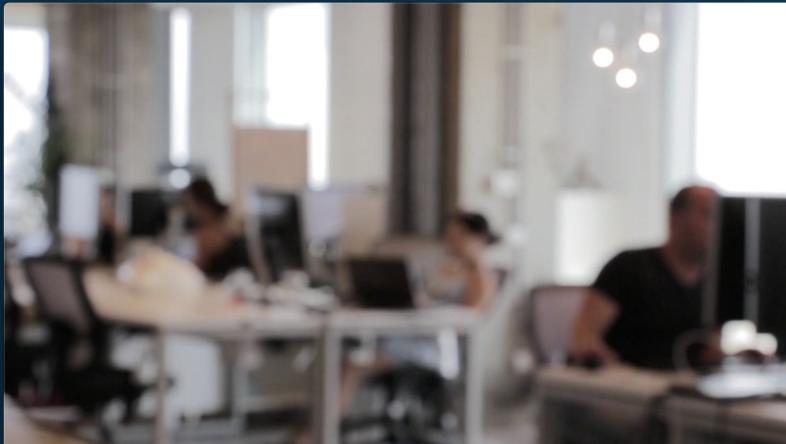
IN EARLY 2020



Users are working in a secure building



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



IN EARLY 2020



Then Covid-19 lockdown happened



All users had to work from home



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

Microsoft | Microsoft 365 SharePoint Plans and pricing More Buy now All Microsoft 🔍

SharePoint

Your mobile, intelligent intranet

See plans and pricing

Watch the video >

Office 365 SharePoint

Team Site

Get started with your site

Share your site. Working on a deadline? Add lists, libraries, and other apps. What's your style? Your site. Your brand.

Newsfeed

Documents

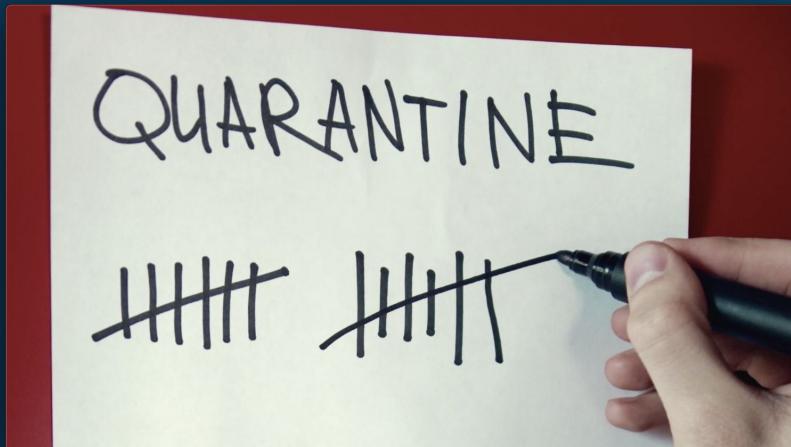
LATE 2020



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



Together with new files that have been created in SharePoint



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

Danger - OneDrive

New Upload

Files > Demo File > Danger

Name	Modified	Modified By	File size	Sharing
file.doc	3 days ago	Guest Contributor	52.5 KB	Shared
Infected.doc	3 days ago	Max Bostall	155 KB	Shared
VirusShare_000001d5dcf754349a66493...	3 hours ago	Justin Rowland	9.45 KB	Shared
VirusShare_000w033ba068501a7fa05fb6...	3 hours ago	Justin Rowland	24.1 KB	Shared
VirusShare_000bb7460c2b987a677ce3...	3 hours ago	Justin Rowland	60.4 KB	Shared
VirusShare_0006cf263ddaa4c493477557e...	3 hours ago	Justin Rowland	15.9 KB	Shared
VirusShare_000caf62715b94e79725b05...	3 hours ago	Justin Rowland	14.4 KB	Shared
VirusShare_0004a48dc6163911f9e959a8b...	3 hours ago	Justin Rowland	16.1 KB	Shared
VirusShare_000e029208e2139e543a0e...	3 hours ago	Justin Rowland	12.5 KB	Shared
VirusShare_000fb9c388053c663491d3d8...	3 hours ago	Justin Rowland	13.1 KB	Shared
VirusShare_000fe225c25ff8b8666f6040c...	3 hours ago	Justin Rowland	106 KB	Shared

Show all

OneDrive

Download

Files > Demo File > Danger

This file is compromised by malware

To protect your PC and other files, we've removed Open, Share, and other commands. You can download this file if you want to remove the malware yourself. Contact your admin for options or learn more.

Download

Name	Modified	Modified By	File size	Sharing
Infected.doc	3 days ago	Justin Rowland	15.9 KB	Shared
VirusShare_000001d5dcf754349a66493...	3 hours ago	Justin Rowland	24.1 KB	Shared
VirusShare_000w033ba068501a7fa05fb6...	3 hours ago	Justin Rowland	60.4 KB	Shared
VirusShare_000bb7460c2b987a677ce3...	3 hours ago	Justin Rowland	15.9 KB	Shared
VirusShare_0006cf263ddaa4c493477557e...	3 hours ago	Justin Rowland	14.4 KB	Shared
VirusShare_000caf62715b94e79725b05...	3 hours ago	Justin Rowland	16.1 KB	Shared
VirusShare_0004a48dc6163911f9e959a8b...	3 hours ago	Justin Rowland	12.5 KB	Shared
VirusShare_000e029208e2139e543a0e...	3 hours ago	Justin Rowland	13.1 KB	Shared
VirusShare_000fb9c388053c663491d3d8...	3 hours ago	Justin Rowland	106 KB	Shared

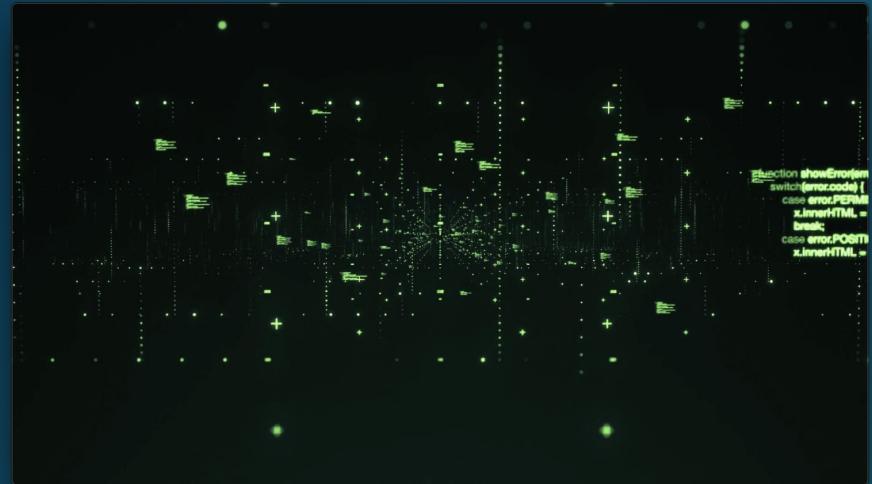
Show all

LATE 2020



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

```
    res.json({ success: false, message: 'Could not register user, username or email might be taken' });
} else {
    res.json({ success: false, message: 'Could not register user, error: ' + err });
}
else {
    sgMail.setApiKey(configSendgrid.SendgridAPIKey);
    fs.readFile("./templates/emailtemplate.html", 'utf8', (err, data) => {
        if (err) {
            if (err.code == 11100) {
                res.json({success: true, message:"Failed with "});
            }
            res.json({ success: false, message: 'Failed to read email file: ' + err });
        }
        data = data.replace("##Title##", "Confirm Account");
        data = data.replace("##Message##", "Please click the button below to confirm your account.");
        data = data.replace("##Link##", host.baseurl + "api/accounts/confirmEmail?token=" + token);
        const msg = {
            to: req.body.email.toLowerCase(),
            from: 'info@codenetic.co.za',
            subject: 'Account Confirmation',
            content: [
                {
                    type: "text/html",
                    value: data.toString()
                }
            ]
        };
        sgMail
            .send(msg)
            .then(() => {
                res.json({ success: true, message: "Email sent successfully" });
            })
            .catch((err) => {
                res.json({ success: false, message: 'Failed to send email: ' + err });
            });
    });
}
```



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

A screenshot of a Windows File Explorer window titled 'Danger'. The window shows a folder structure under 'Downloads' on 'This PC'. Inside the 'Danger' folder, there are several files: 'file.doc', 'Infected.doc', and several VirusShare files. One of the VirusShare files is highlighted, showing its details: Name: 'VirusShare_000001c1d5dd7f45...', Date modified: '6/15/2020 1:50 PM', Type: 'Microsoft Word 97...', Size: '155 KB'. The status bar at the bottom indicates '5 items 1 item selected 154 KB'.

A screenshot of a Microsoft OneDrive web interface titled 'Danger'. The interface shows a list of files in a folder. The files listed are: 'file.doc', 'Infected.doc', and several VirusShare files. The 'Infected.doc' file is highlighted, showing its details: Name: 'Infected.doc', Modified: '3 days ago', Modified By: 'Max Bassell', File size: '155 KB'. The status bar at the bottom indicates '5 items 1 item selected 154 KB'.



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

1



Proxy with ICAP
Protocol

2



AntiVirus

3



Glasswall
Proxy Server

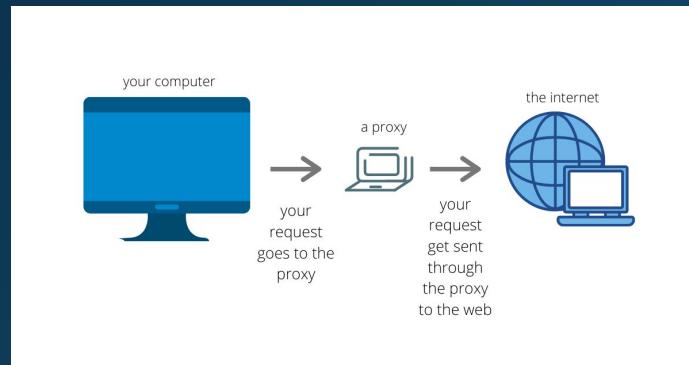
1



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
POWERED BY BIGPOINT

Barracuda

COMODO
Certification Authority
POWERED BY ECTO

GARRISON
TECHNOLOGY

WatchGuard

2



AntiVirus



Check for known bad files

Danger - OneDrive

glasswallsolutionsltd-my.sharepoint.com/personal/jrowland_glasswallsolutions_com/_layouts/15/onedrive.aspx?originalPath=aHR0chHM6Ly7nbGfz3dhGcz21dGlvbNsdGQtbXuz2hcmVwh2J...

McAfee® | WebAdvisor

Download

Files > Demo File > Danger

Name	Modified	Modified By	File size	Sharing
file.doc	3 days ago	Guest Contributor	52.5 KB	# Shared
Infected.doc	3 days ago	Max Bussell	155 KB	# Shared
VirusShare_000a033ba068501a7fa2b6fb6...	5 hours ago	Justin Rowland	24.1 KB	# Shared
VirusShare_...	5 hours ago
VirusShare_...	5 hours ago
VirusShare_000ca62715d804e79725b0b5...	5 hours ago	Justin Rowland	14.4 KB	# Shared
VirusShare_000d4bde16
VirusShare_000e0229208c62139c6543e0...	5 hours ago	Justin Rowland	12.5 KB	# Shared
VirusShare_000fb36c388053c66341fd3d8...	5 hours ago	Justin Rowland	13.1 KB	# Shared
VirusShare_000fb22525ff8b6666f6040fc...	5 hours ago	Justin Rowland	100 KB	# Shared

Woah, that download is dangerous!

We found that there might be viruses, spyware, or other potentially unwanted programs in the file you're trying to download.

Filename: Infected.doc
Domain: glasswallsolutionsltd-my.sharepoint.com

Accept the risk Block download

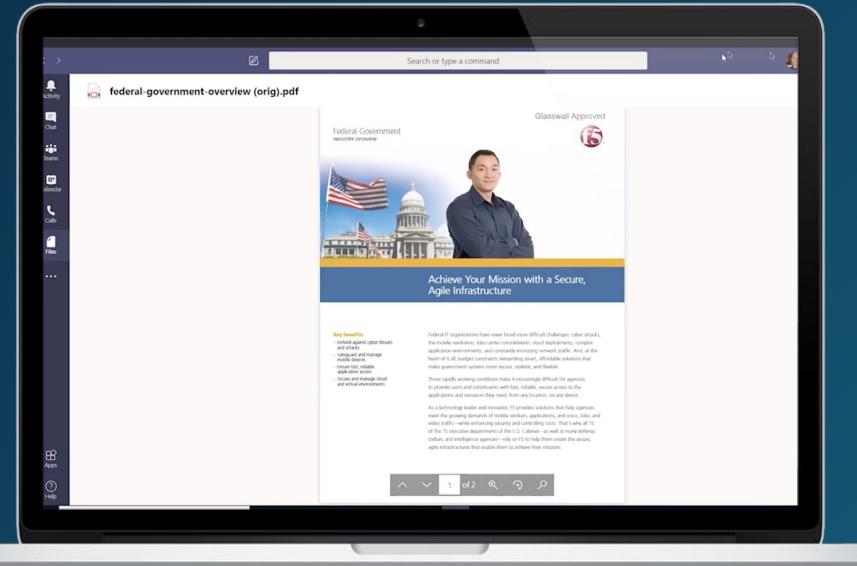
3



Glasswall
Proxy Server



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



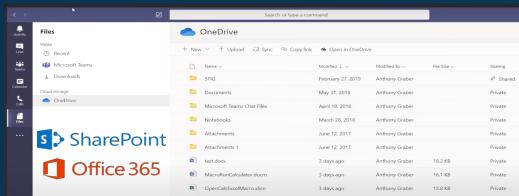
Supported File Types

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

Rebuilding into known good

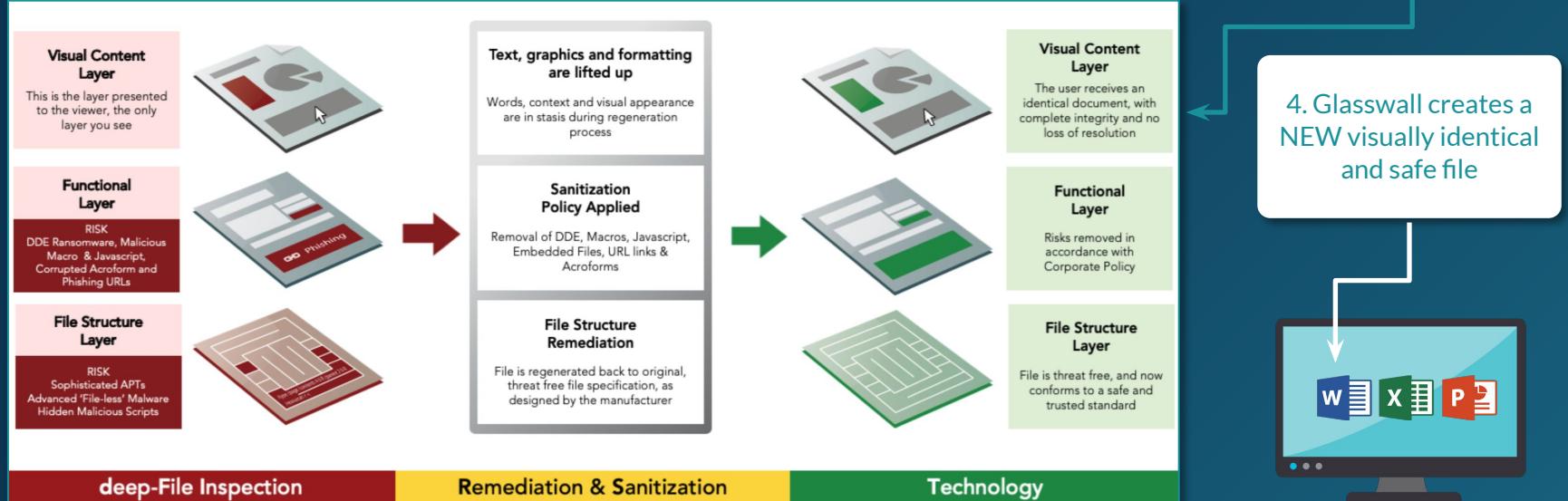


1. Files in storage could be malicious



2. Instead of looking for bad

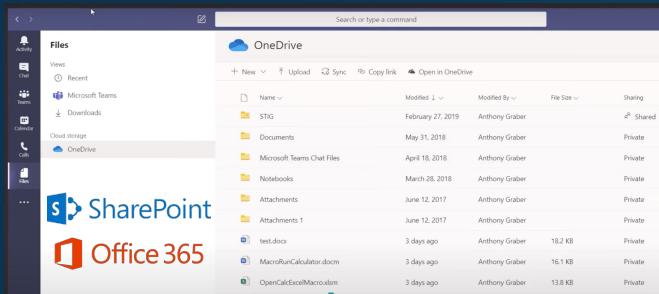
3. Rebuild file into a known good state



Solution workflow



1. User clicks on files stored on SharePoint



I don't have to worry about this file



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



3. and sends them to malware detectors and Glasswall



GLASSWALL

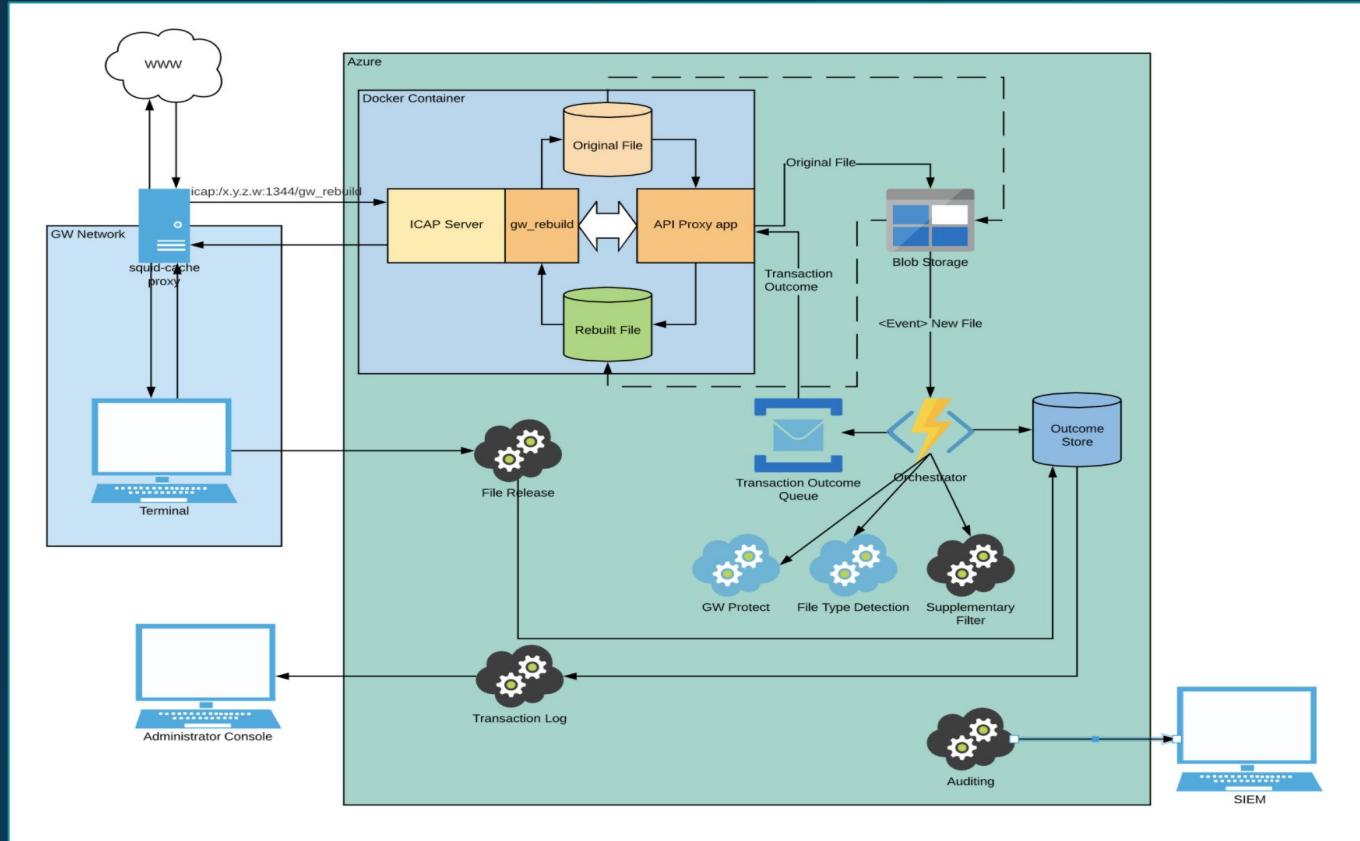
Anti-virus

CDR



4. Glasswall creates a NEW visually identical and safe file

Cloud based Architecture (Azure)





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)





PROXY SERVER

SHAREPOINT CASE STUDY

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



GLASS WALL

Thanks