GLASSWALL

Safety and Integrity
Through Trusted Files.

Redacted Customer

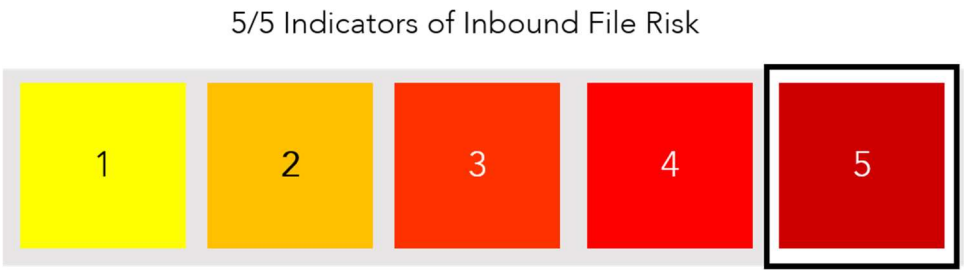
File Risk Report

FileTrust™ for Email

Executive Summary

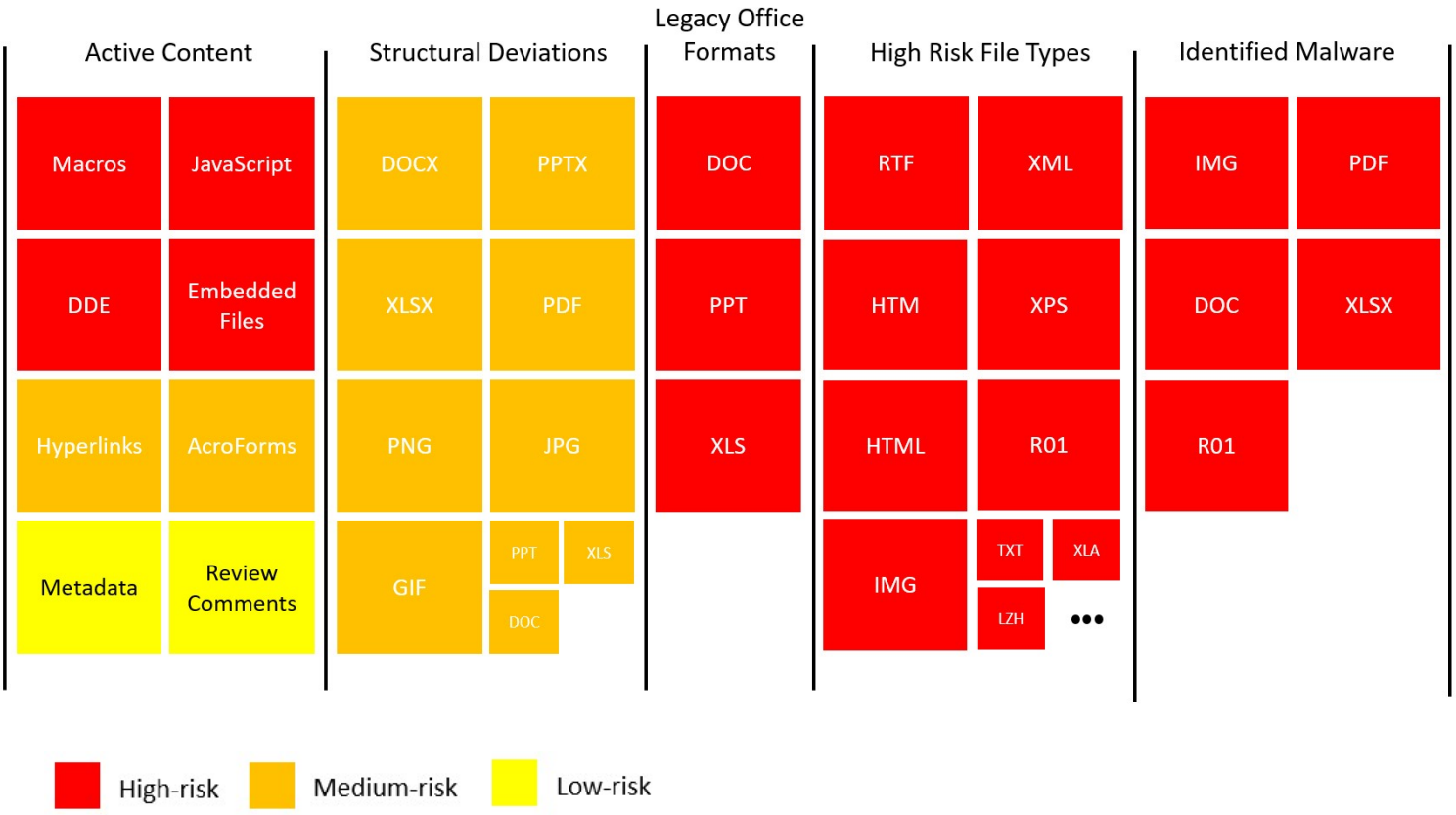
Redacted Customer's inbound email risk has been assessed for the following:

File Risk Indicators	
High-risk Active Content	!
Structural Deviations	!
Legacy Office Formats	!
High-risk File Types	!
Identified Malware	!



Risk Breakdown

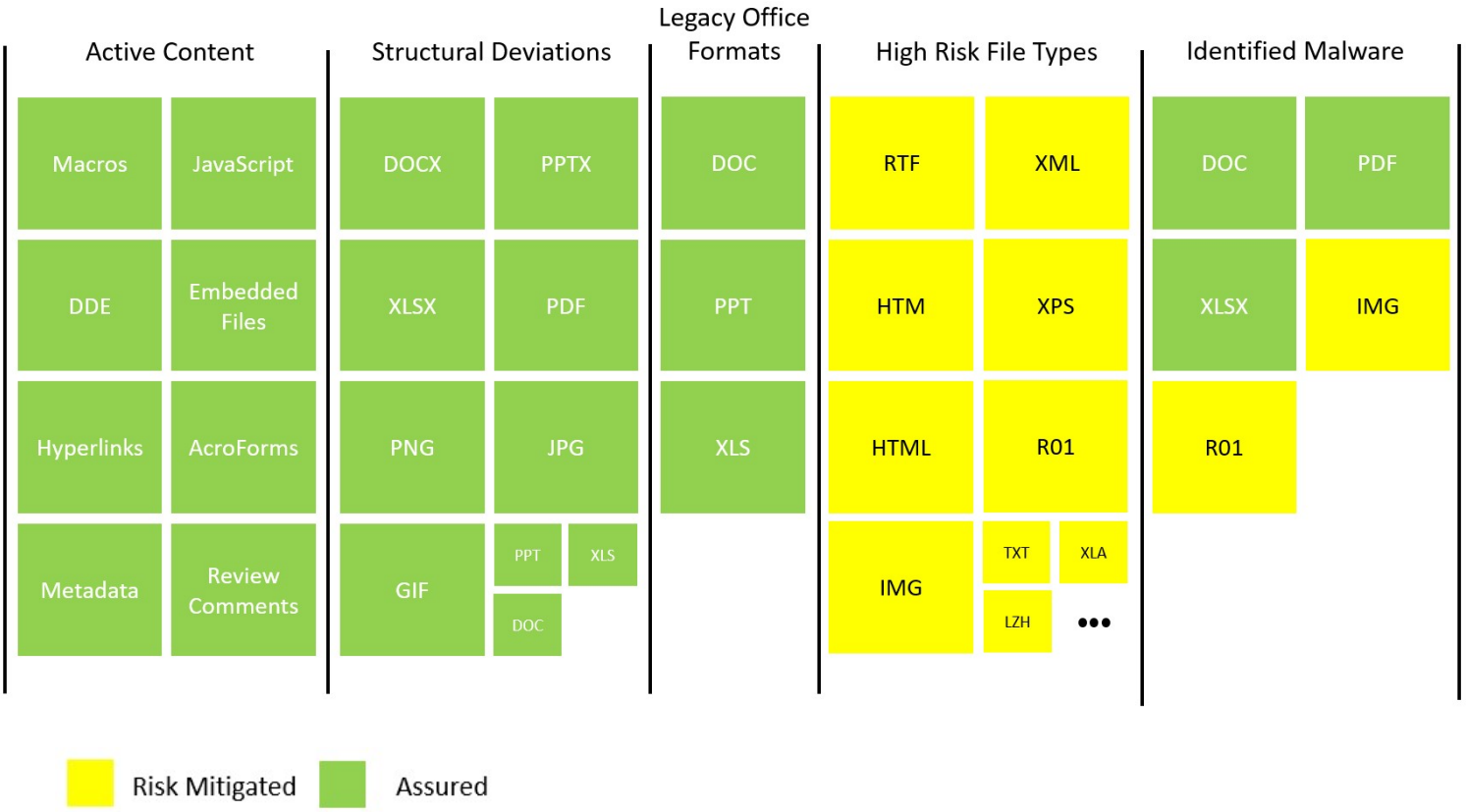
Glasswall identified the following elements of risk. These elements are divided into sections that are further detailed in the main body of the report.



Glasswall Risk Management

The primary value of Glasswall is the ability to expose and manage the risk from business files. Unknown malware is disarmed before AV/Sandbox technologies become aware of the threat.

With Glasswall, Redacted Customer's risk profile would be improved as follows:



- Active Content would be sanitised (removed) from files through the application of policy, restricting features to only those users that need them for specific business reasons. Users would not be exposed to unnecessary risk from Active Content they do not require.
- Business documents would be validated against the 'known good' specification with structural deviations remediated (repaired), mitigating the risk of structural based malware.
- Legacy Office formats are remediated and sanitised.
- Glasswall would provide visibility and tooling to control which types enter the organisation. Users would only receive files types compliant with corporate policy.

Introduction

Glasswall's unique deep-File Inspection, Remediation and Sanitisation Technology (d-FIRST™) creates safe, compliant and visually identical files that are free from the risks of malware. Both Gartner and NCSC advise that techniques such as Glasswall d-FIRST™ should be used as a defence against malware for file and document ingress. The objectives of the report are as follows:

1. Quantify the risk of Active Content to users.
2. Expose the extent to which files and documents deviate from their known good specification.
3. Provide visibility on all file types entering the organisation.
4. As a measure of the effectiveness of the current security protections, report any malware, both known and unknown.
5. Give security personnel operational experience of FileTrust™ for Email.

The report covers a 6-month period, analysing real-time copies of production email traffic:

No. Users in Sample	No. Emails
~2,000	145,796
No. Files	**Active Content Identified (Items)**
344,827	104,641
Files Remediated/Sanitised	**Upstream Security Products**
48.95%	Proofpoint, FireEye
Unknown Malware Disarmed	**Known Malware Disarmed**
24	6

The results can be further broken down into five categories:

Active Content - Structural deviations - Legacy Office formats
High-risk file types - Identified malware

Active Content

Active Content such as macros, JavaScript and embedded files, are often manipulated to trigger malicious payloads. Glasswall sanitises (removes) these features from files. Exposure to these features can be managed by policy, effectively reducing risk while supporting operational efficiency. Policy rules may, for example, be set to allow recipient to receive macros from trusted senders where they need this Active Content to effectively perform their jobs. This gives complete, granular control over the Active Content entering the organisation, thereby greatly reducing exposure to unnecessary risk.

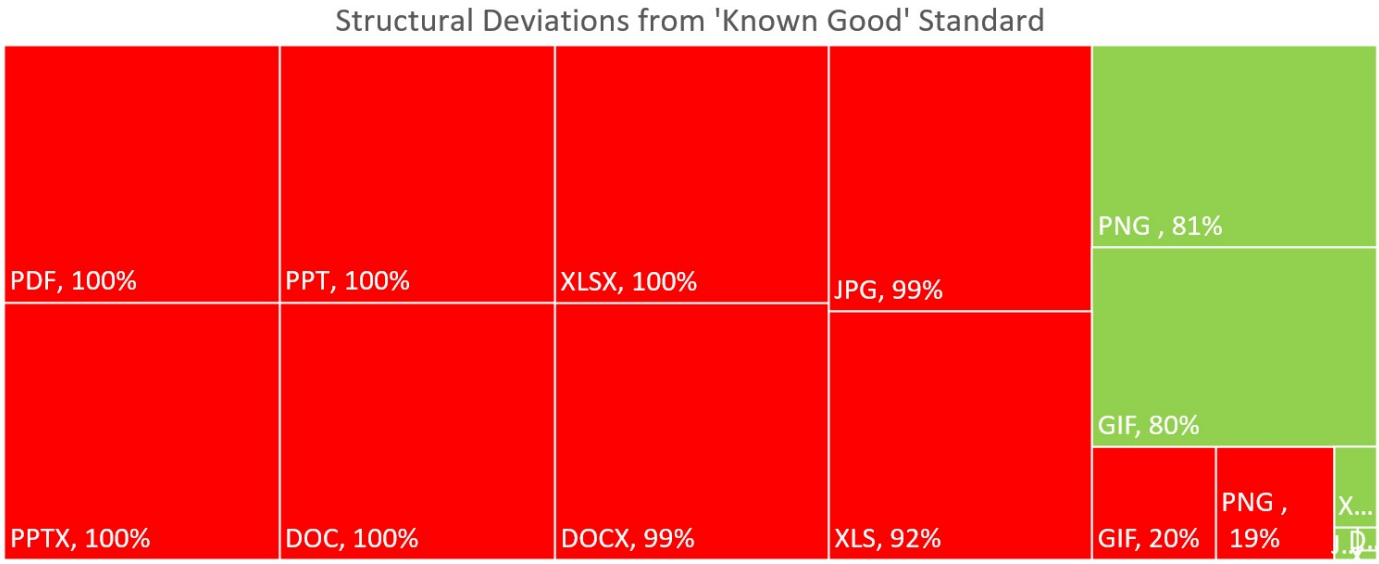
The following Active Content was identified and was not removed or disarmed by existing layers of protection.

Threat	No.	Risk	Common Related Malware
JavaScript	314	High	Cerber Ransomware, Kovter, StalkDaily Worm, Locky, Emotet
Embedded Files	6,782	High	WannaCry, Emotet
Macros	485	High	Agent Tesla, Trickbot, Gandcrab 5.2 Ransomware
DDE	0	High	Admind, nanocore, Locky
Hyperlinks	21,316	Medium	Emotet, Phishing, can be spoofed to point to malicious links
AcroForms	2,552	Medium	Allow for auto execution within pdfs
Metadata	73,339	Low	Surveillance
Review Comments	0	Low	Surveillance

Structural Deviations

Glasswall regenerates files to the safe standard of 'known good', enforcing the format's structural specification. Each structure in a file is validated against its specification, any that fails validation is marked as non-conforming. Remediation repairs these non-conforming structures, bringing them back into line. This is done for all the structures in the file and a regenerated file structure is compliant and standardised. The by-product is that any malware that is hidden or obfuscated in the file structure is either disarmed, destroyed or removed.

The following file types carried structural deviations from their 'known good' Standards:

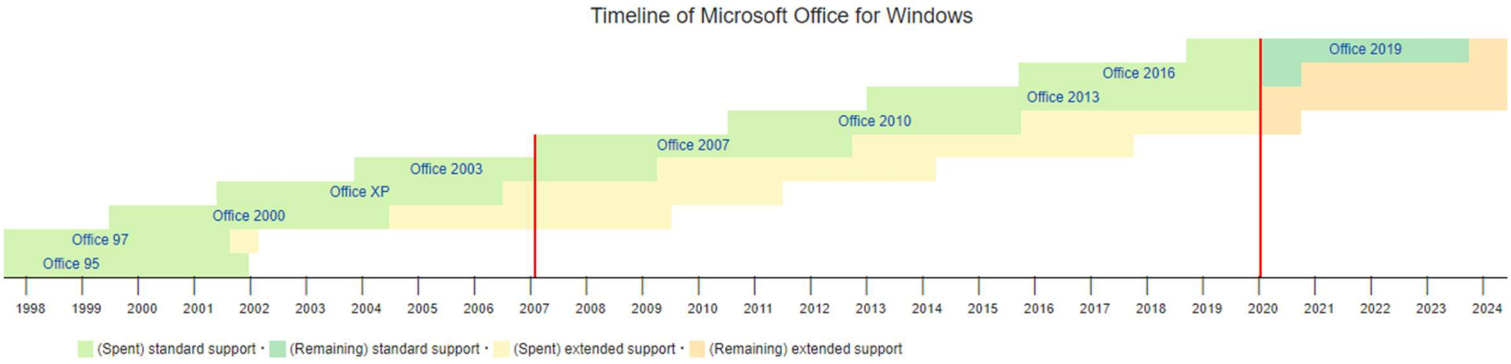


Glasswall's research shows that 93% of files and documents carry structural deviations from their 'known good' specification. These structural deviations represent significant risk. Essentially, they are places in which malicious code can be hidden.

See the Appendix for additional information regarding 'known good' file specifications.

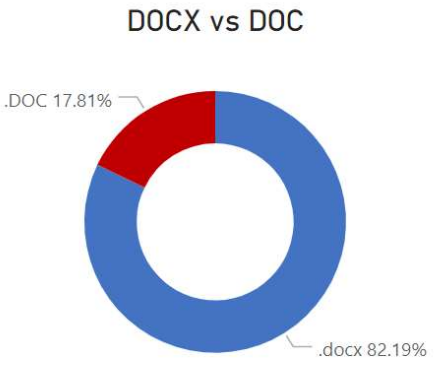
Legacy Office Formats

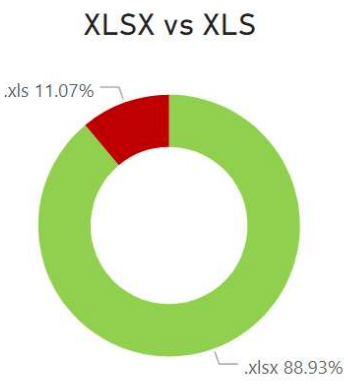
The first version of Word, released in 1983, was for the MS-DOS operating system.
Initially, it implemented the proprietary binary .doc format. However, Word 2007 deprecated this format in favour of Office Open XML (.docx .xlsx and .pptx).

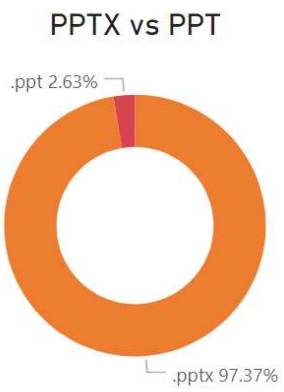


Legacy Binary .doc .xls or .ppt files are an unnecessary risk for any organization. There's no sensible reason to use these old file types when the far considerably safer XML formats have been available for over a decade. There are a considerable number of known vulnerabilities for these unsupported formats, which are still being exploited today.

The following Office file formats were identified:







Glasswall regenerates binary Office files to the safe standard of 'known good', enforcing the format's structural specification and eradicating high-risk Active Content, mitigating the risk from Legacy Office formats.

High Risk File Types

Glasswall provides visibility and tooling to control which file types can enter the organisation. Users only receive files types compliant with corporate policy.

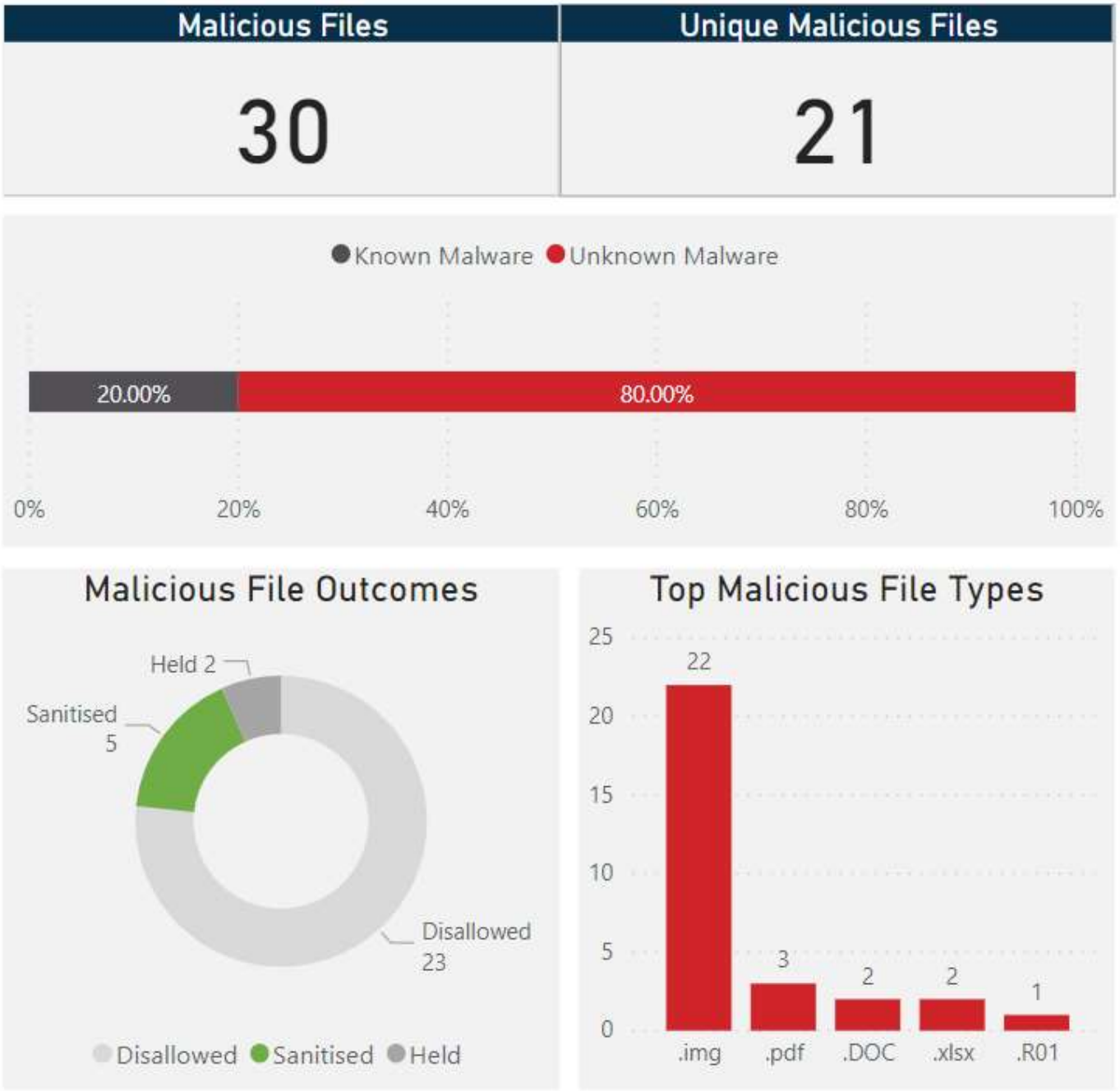
The following additional file types were identified:

File Type	No.	Risk
.html	500	High
.txt	334	High
.htm	208	High
.img	15	High
.xml	7	High
.xps	6	High
.rtf	4	High
.xla	3	High
.lzh	1	High
.R01	1	High
.ics	579	Low
.dat	89	Low
.bmp	71	Low
.emz	65	Low
.CSV	60	Low
.zip	56	Low
.dmr	55	Low
.p7s	43	Low
.mso	25	Low
61 additional file types...		

File types are deemed high risk due to having known malware examples within the Glasswall Threat Intelligence data set.

Identified Malware

Glasswall Threat Intelligence, reports over time on files that have identified as containing malware. The service provides a metric for the effectiveness of Glasswall FileTrust™ for Email's unique capability to disarm malware.



The industry took on average 4.23 days to identify unknown malware that had been made safe by Glasswall.

Appendix

File Specifications

The Glasswall process can be applied the following 28 file types.

Category	File Type	Extensions
Microsoft Office (Legacy)	Microsoft Word	doc, dot
	Microsoft Excel	xls, xlt, xlm
	Microsoft PowerPoint	ppt, pot, pps
Microsoft Office (2007+)	Microsoft Word	docx, dotx, docm, dotm
	Microsoft Excel	xlsx, xltx, xlsm, xltm
	Microsoft PowerPoint	pptx, potx, ppsx, pptm, potm, ppsm
PDF	Adobe PDF	pdf
Images	JPEG	jpeg, jpg, jpe
	PNG	png
	GIF	gif

Microsoft Office binary file type specifications can be found in the following location:
https://msdn.microsoft.com/en-us/library/office/cc313105(v=office.12).aspx

Microsoft Office XML file type specifications can be found in the following location:
https://msdn.microsoft.com/en-us/library/gg548604(v=office.12).aspx

PDF file type specification:
https://www.adobe.com/content/dam/acom/en/devnet/pdf/pdfs/PDF32000_2008.pdf

Glasswall Documentation

The following link provides detailed FileTrust™ for Email documentation.
https://docs.glasswallsolutions.com/