Glasswall Threat Intelligence

The Glasswall Engine looks deep into the DNA of a document and identifies active content and broken structures that represent risk to the user that chooses to open a document. Glasswall provides unique insights into file-based threats and how risks may accumulate across your organization as a result. Security teams can make intelligent policy decisions on active content types such as Macros in Office or JavaScript in PDF documents. Glasswall is also able to check every file against over 50 Reputation Services and Threat Feeds from a database of over 12 billion goodware and malware files.

Key benefits

- ✓ In-depth CDR based risk analysis of documents that surpasses signature-based feeds
- ✓ Identify risks relating to active content and broken document structures which may result in infection
- ✓ 50 Reputation Services and Threat Feeds from a database of over 12 billion goodware and malware files

Key features

- Identify active content risks from JavaScript, Macros, Acroforms, Dynamic Data Exchange, Embedded Files, Embedded Images, External Hyperlinks and Internal Hyperlinks
- Review Comments and Metadata due to CDR analysis which looks deep in each file
- Confirm malware identification from a database which grows by 8 million files daily
- Benefit from malware identification in brand new and polymorphic threats

Use cases

- Email Security for file attachments
- Files at rest and in transit - crossing trust boundaries and with potentially unknown provenance
- Assessing backup health and integrity before restore to clean environment
- Efficacy validation of other solutions in the security stack whilst benefiting from full file protection with CDR
- Trend analysis

How it works

Glasswall provides deep file analysis from its Content, Disarm and Reconstruction (CDR) engine to identify potential inbound risks as part of each file inspection. Theoretical and actual risks are neutralised in milliseconds as part of the CDR process, with telemetry relating to trends being surfaced to help security teams stay on top of threats. Reputation services and Threat Feeds augment the solution to positively affirm malware that has already been sanitized by the Glasswall Engine, ensuring that security teams can understand the value being obtained from substitute solutions which promise lower efficacy.

Structural deviations

Active content

Legacy Office formats

High risk file types

Identified malware

GLASSWALL

glasswall.com
info@glasswall.com