DISA Technical Exchange Meeting

Glasswall Zero Trust & Intelligent File Protection

8th July, 2025

Team

Paul Farrington – Chief Product Officer – 4 years – pfarrington@glasswall.com

Marc Robinson – Chief Technology Officer – 3 years – mrobinson@glasswall.com

Kelly Davis – Sr. Solution Architect – 3 years - kdavis@glasswall.com

Sam Hutton – Chief Revenue Officer – 10 years/Co-founder – shutton@glasswall.com

Chris Wyman – DOD Sales Director – 1 year – cwyman@glasswall.com

Weaponized Files Undermine Mission Assurance

File-based threats are a top vector for cyberattacks

Malware, ransomware, steganography, and hidden exploits frequently enter networks via seemingly legitimate documents

Over 90% of successful cyber attacks begin with a file-based vector, often bypassing traditional detection tools*

Traditional detection-based security is increasingly ineffective

Signature and heuristic detection cannot keep pace with zero-day, polymorphic and AI-generated threats

12,000 new malware variants are created every hour.# Adversaries in nation-state campaigns craft custom payloads to evade antivirus and sandboxing solutions^

High-consequence environments cannot afford even a single failure

A single compromised file can disrupt critical missions, compromise sensitive data and threaten lives

DOD and intelligence community mandates (NSA Raise the Bar, NCSC guidance) emphasize zero trust, “never trust, always verify”, **files are no exception**±

*Verizon DBIR 2023, #AVTEST, ^MITRE ATT&CK Framework, ±(DODI) 8540.01

GLASSWALL

Glasswall exists to remove all file-based threats – *critically* for those that evade detection

Premier provider of **Zero Trust Content Disarm and Reconstruction (CDR)**

File sanitization capabilities

- ✓ Disarms malware threats in complex files
- ✓ Neutralizes structural file malformations
- ✓ Enables content redaction
- ✓ Defeats hidden data exfiltration
- ✓ Mitigates Steganography
- ✓ Sub-second processing
- ✓ Custom policy enforcement
- ✓ Scales from laptop to enterprise
- ✓ Provides advanced risk reporting

Trusted by Governments

Credentials

- ✓ Top performing CDR – Advanced Level 3
- ✓ NSA Raise The Bar mandated solution – NCDSMO
- ✓ Top rated malware content filter by NCDSMO
- ✓ Customer list includes 5 Intel agencies
- ✓ Deployed 7+ years
- ✓ CMMC Level 1, with Level 2 *In Progress (Oct '25)*
- ✓ Securely developed using DISA STIGS
- ✓ Published Software Bill of Materials (SBOMs)

Glasswall's Zero Trust & Intelligent File Protection

1. Inspect

Breaks down the file into its constituent components. Validates file's structure against its specifications

2. Rebuild

Non-conforming file structures that fail validation are rebuilt in-line with the file's specifications

3. Clean

Removes high-risk file structures that contain active content, based on configurable policy

4. Deliver

Semantic checks ensure the file's integrity. The safe and visually identical file is now ready to use

Capabilities

Risk Analysis

Provides security teams with detailed reporting of all content discovered while Glasswall is inspecting a file

Transform to JSON/XML

Transforms complex data formats into more simple/verifiable ones (JSON/XML) and reconstitutes them. This capability exposes a file's internal structure, enabling third parties to carry out hardware/software syntactic and semantic verification

Data Loss Prevention (Find and Redact)

Gives security teams the capability to specify forbidden words. Glasswall analyses a file and identifies forbidden words, and then enacts the user defined policy

Risk Removal (CDR)

The core capability of Glasswall, developed to disarm malicious files, returning them to their manufacturer's known-good file specifications

Intelligent Threat Prediction (Foresight)

Based on the data objects surfaced and telemetry created during the CDR analysis phase we can accurately predict the presence of malware based on machine learning & AI

Steganography Prevention

Use of file bouncing, palette shuffling and image smoothing of edge pixels to provide full mitigation of steganography techniques

Active Content Risk

Acroforms

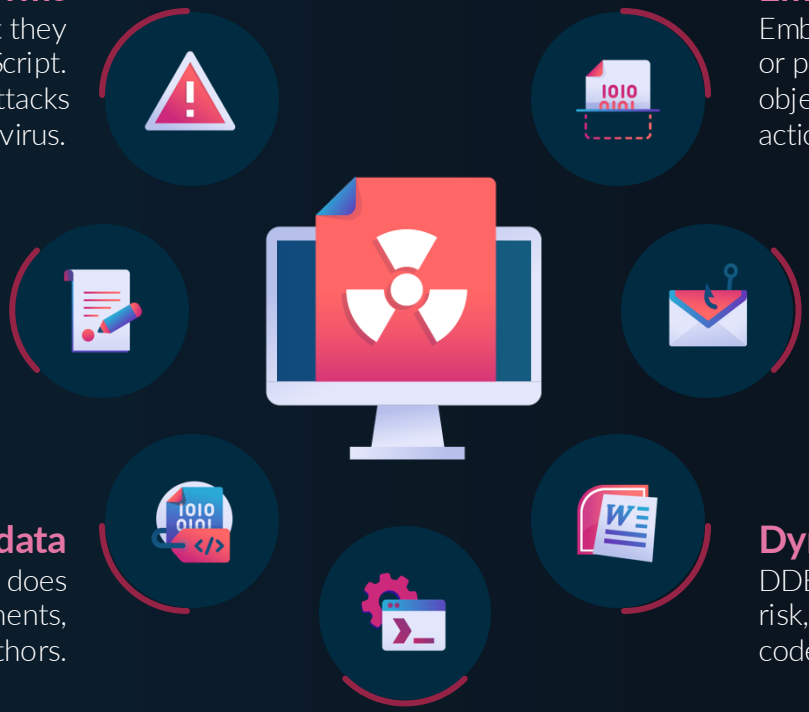
'Acrobat Forms' look just like any other form, but they may also contain active code such as JavaScript. This active code can be exploited to launch attacks commonly missed by traditional Antivirus.

Digital Signatures

Whilst the signing may not represent a threat, if the ownership and trust of the certificate chain has been compromised, this could trick a user into opening a document that contains something malicious.

Review Comments and Metadata

Metadata can contain information an organization does not wish to disclose publicly. Such as review comments, tracked changes, and the names of the file's authors.



Embedded Objects

Embedded objects within files can be used to hide data or provide a way for active code to be triggered. These objects are often harnessed by bad actors to perform actions without a user's permission or knowledge.

Hyperlinks

Hyperlinks are commonly used in targeted phishing attacks. While links may appear innocent on the surface, the link itself may take the user to a different destination, designed to start a chain of malicious events.

Dynamic Data Exchange (DDE)

DDEs within Microsoft documents are known to present risk, as the protocol may be used to execute malicious code on the recipient's computer.

Macros and Scripts

Forms of active code. These extra file functions can perform actions without a users' permission. Starting a chain reaction of malicious events. Often used by bad actors to mount an attack against the user or receiving system when expressed in a business document.

Structural Risk

Example:

Digital Polyglot:

- A single file crafted to be interpreted as **multiple formats** by different applications (e.g. Adobe Acrobat, 7-Zip)
- Contains many valid headers and structures, allowing it to behave like a mix of file types
- Malicious content can evade detection because each tool only analyzes the format it recognizes
- With a blueprint of where polyglots hide, Zero Trust Content Disarm and Reconstruction (CDR) safely rebuilds polyglot files and removes the risk

Use Cases & Solutions

Cross Domain Solutions

Use Cases

- CDS deployments
- Data diode integration
- Secure data transfers across domains
- Custom file processing flows, including multi-processing support
- Disarm files
- Remove hidden data

Custom integration with system integrators via our SDK

Embedded Engine

Scaled File Processing

Use Cases

- Secure file upload & download - REST API
- OneDrive & SharePoint
- Document gateways & web appliances
- Cloud storage container processing
- Network proxy integration via ICAP
- Disarm files and validate XML data
- Remove hidden data

Integrates via Sync and Async API endpoints

Glasswall Halo

User Centric Cloud & Isolated File Processing

Use Cases

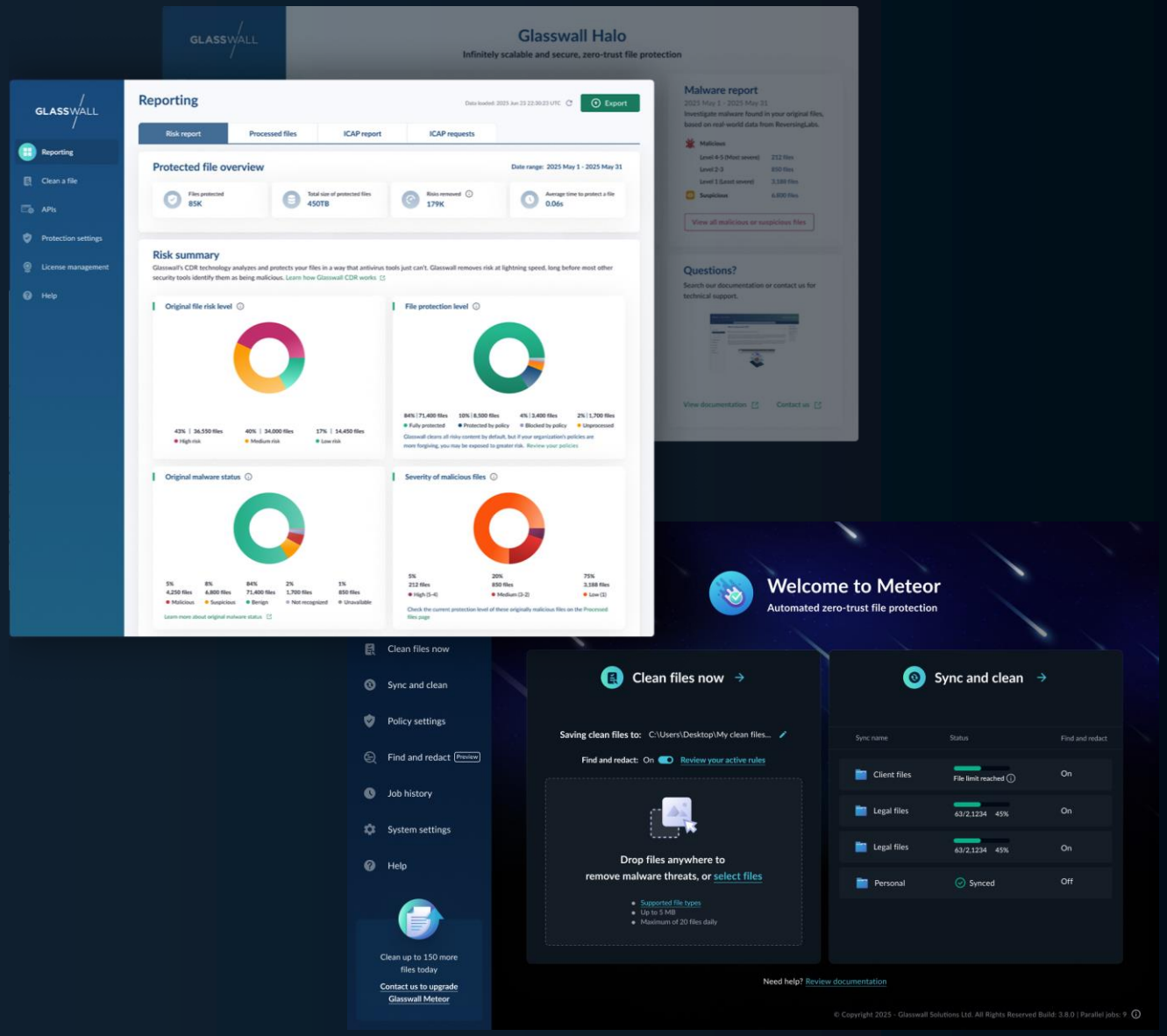
- Local & tactical deployments
- Secure local & cloud folder support
- Find & redact content
- Isolated VM and edge device compatibility
- Disarm files
- Remove hidden data

Application connects with 200+ cloud storage providers

Glasswall Meteor

Product Demos

- Glasswall Halo
- Glasswall Meteor



Technology & Deployments

Embedded Engine
Cross Domain Solutions

Deployment

- On vendor / SI appliances
- Custom, code-level integration
- Multi-language SDKs – C#, C++, Python, Java

- Multiple Linux Distro and Windows OS support

Glasswall Halo
Scaled File Processing

Deployment

- API-first, scalable, container-based architecture
- Support for SSO OIDC IDP – AuthZ/N
- Dashboarding, reporting and integration with log aggregators
- DISA STIG, CIS, SBOMs, SAST, SCA
- **On-prem, virtual appliances**

- **Multi-cloud – JWCC / Gov / IL5-6**

Glasswall Meteor
User Centric Cloud & Isolated File Processing

Deployment

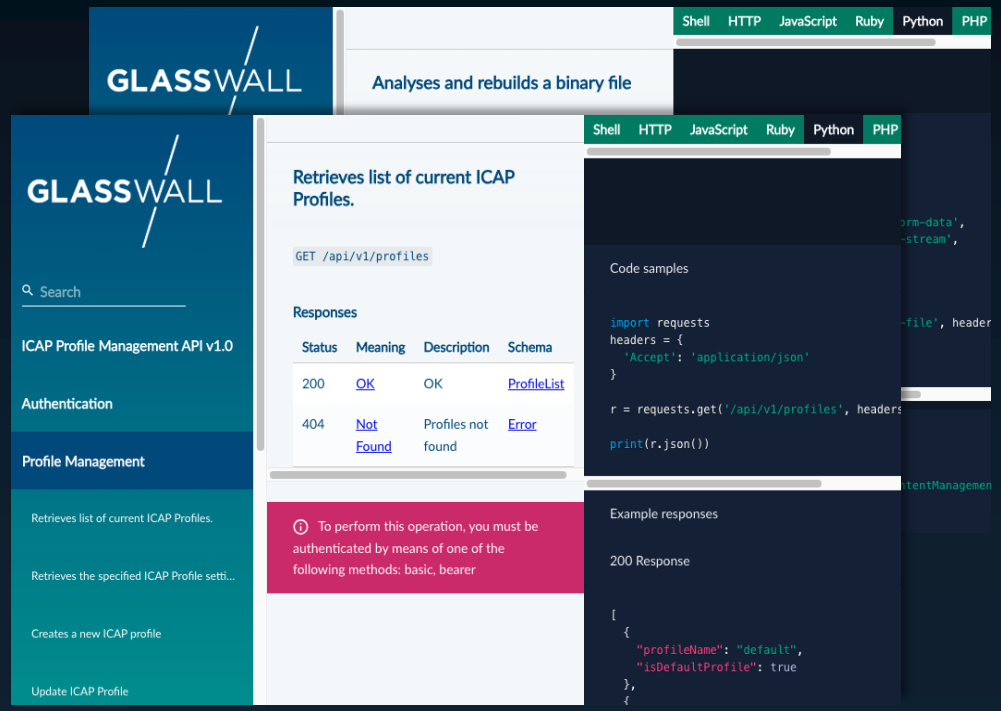
- Tactical, laptop, desktop & server deployments
- Isolated VM and edge device compatibility
- Native Windows Desktop / Server or VM installation

For all solutions, internet not required during deployment or operation

API Integration

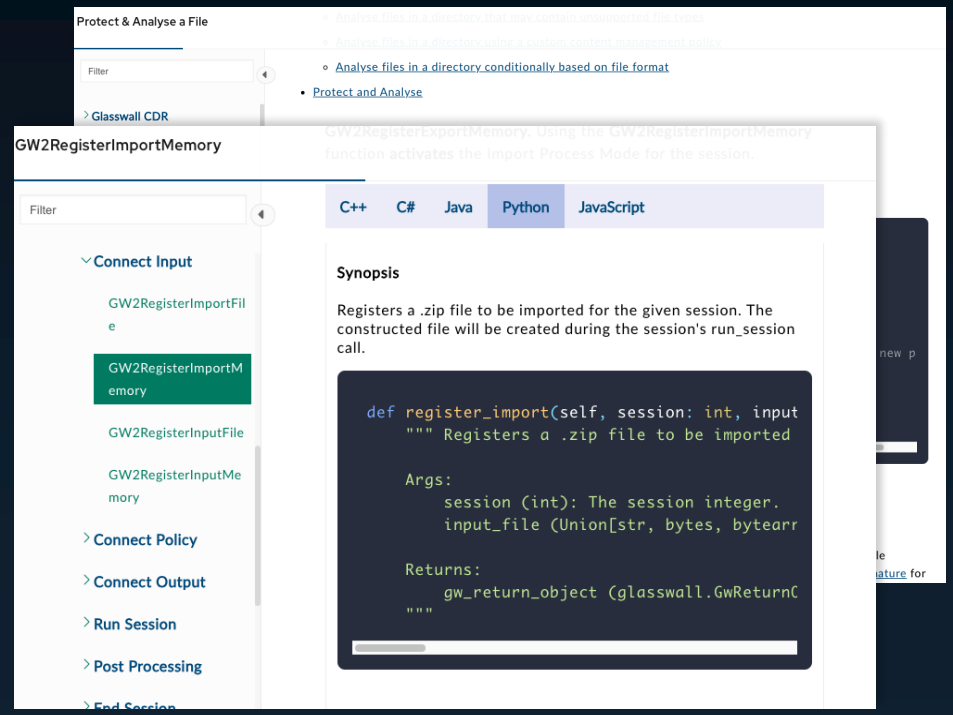
Glasswall Halo

REST API



Embedded Engine

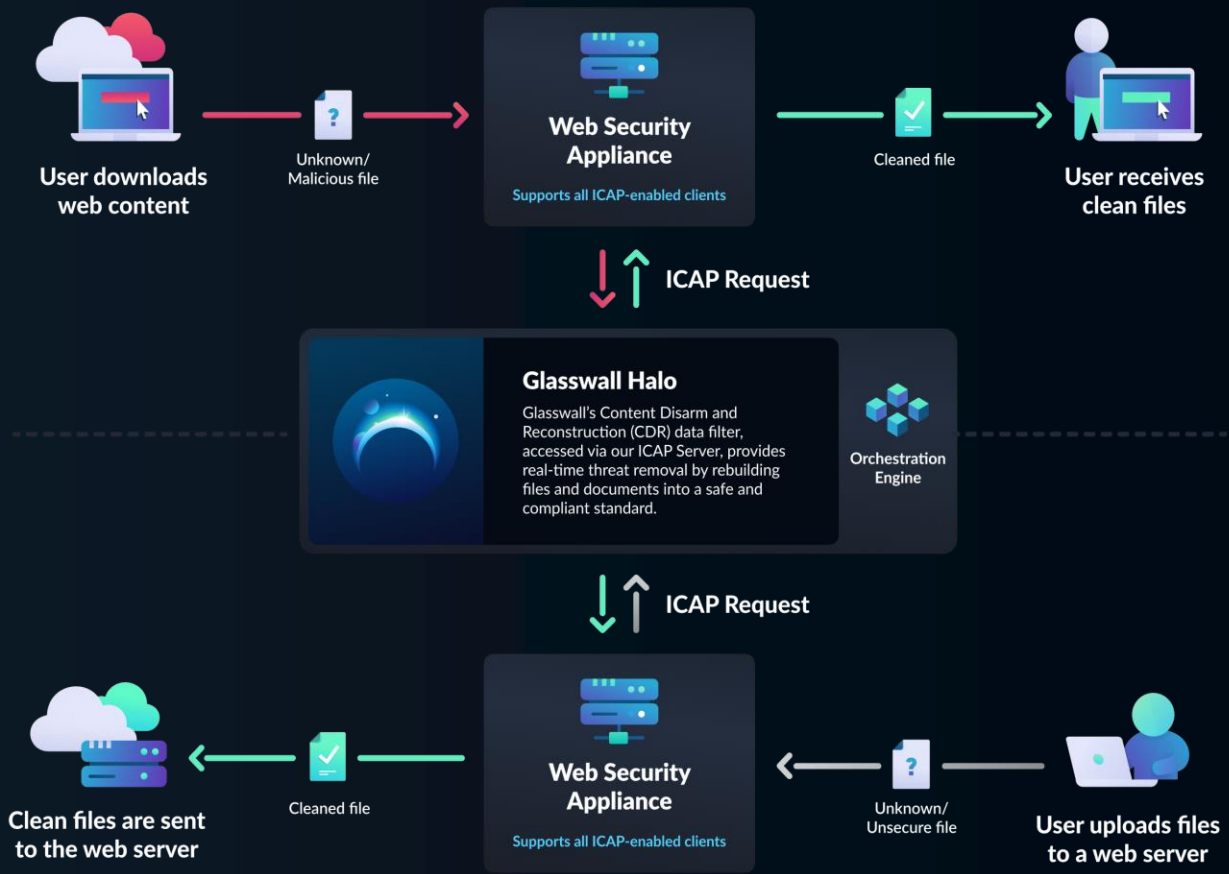
Application API



Glasswall Halo

Remote Browser Isolation (RBI) Enabler via ICAP

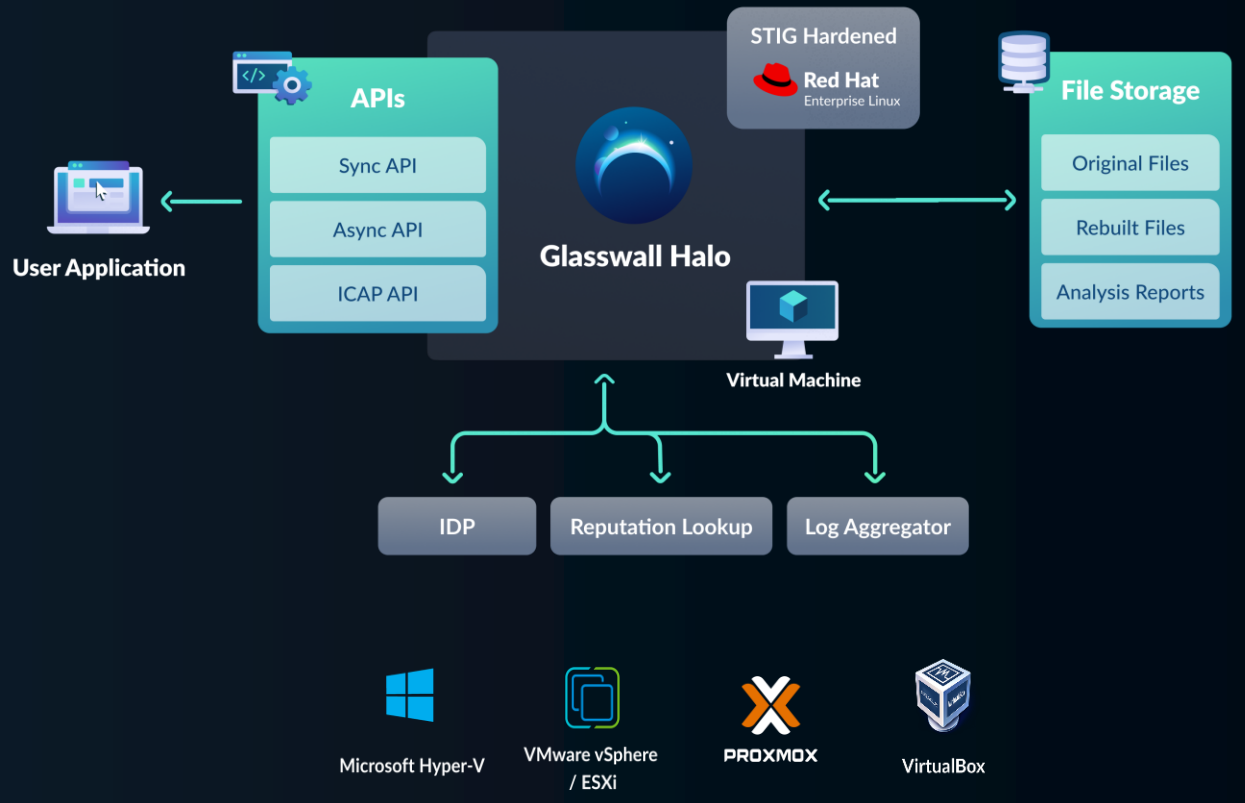
- Deployment via network appliance for seamless protection of web traffic
- Highly configurable based on media types
- Compatible with any ICAP-enabled network appliance
- Detailed configuration guidance for F5, Fortigate and proxies



Glasswall Halo

Deploy as standalone virtual appliance or scale set

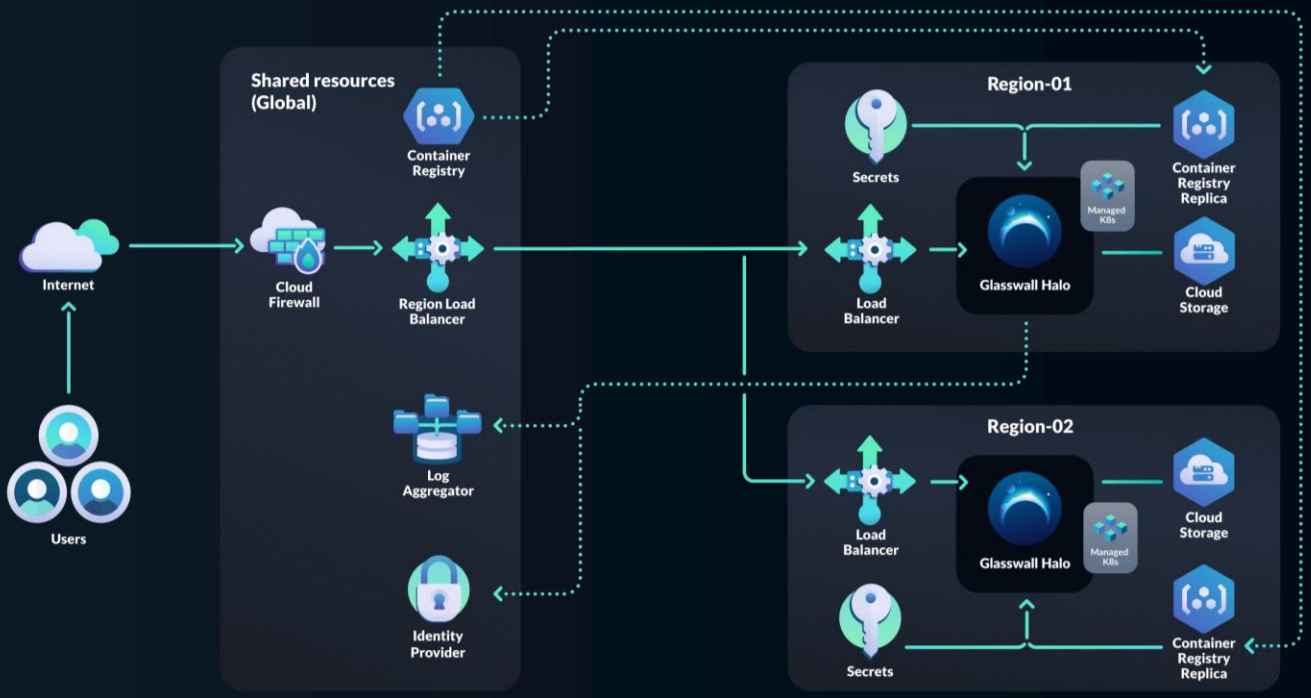
- Ideal for **on-premise or air-gapped environments** where utilization of cloud infrastructure prohibited
- Deployment is simple via **preconfigured VM images**
- DISA STIG hardened and maintained images
- SBOMS and vulnerability data disclosed on request



Glasswall Halo

Deploy as part of a scalable cloud solution using managed Kubernetes

- All common managed Kubernetes platforms
- *Limitless* scale - horizontally and vertically
- Patterns and configuration with proven compatibility with IL5/6 services and restrictions
- Air-gap deployment options



JWCC multi-cloud support

Azure AKS | AWS EKS | Oracle OKE | Google GKE

Glasswall Halo

Industry-leading performance

Sub-second Processing

Cleans files in less than a second
(Mean file processing speed: 38 ms)

API success rate

99,999%

Example

Five workload node pool

Throughput	Files processed	GBs processed
Per hour	93,800	343
Per day	2,250,000	8,230

50 CDR Engines
16 virtual cores per node - 80 total
56 GB Memory per node - 280 GB total

Further data: https://docs.glasswall.com/docs/performance-summary

Cluster configuration assumes specific memory and compute allocations for containers. Production performance will ways depend on size and complexities of real-world files. Configurations can be optimized to favour throughput or file processing speeds.

20 business files ranging from 17 MB to 0.05 MB in size

- File types include: PowerPoint, Video, Excel, Word, Image, PDF, Audio
- Mean file size = 3.74 MB
- Median file size = 0.64 MB
- 5 Engines per node
- Request concurrency to availability of resource is 1:1

Creating Value For Operational Teams

Proactive, Zero Trust-aligned protection

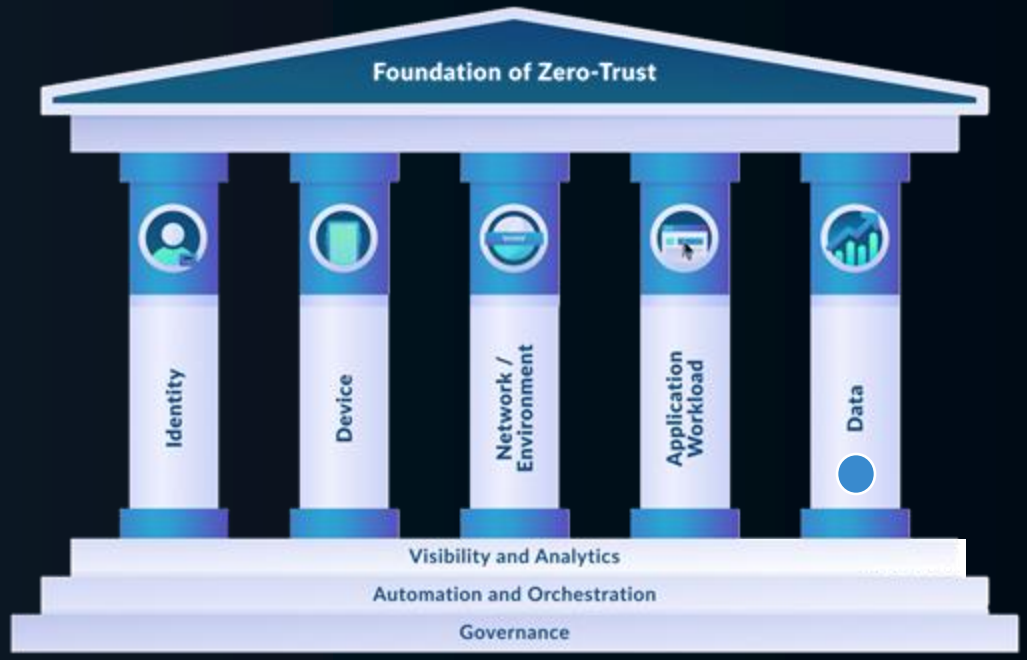
- Sanitizes every file before entry, blocking external threats and insider exfiltration.
- Fully Zero Trust, preventing malicious content even in disconnected or contested environments.

Modular, scalable, rapidly integrable

- Flexible architecture integrates quickly into tactical and enterprise networks.
- APIs enable seamless adoption, accelerating secure deployment.

Flexible deployment for any mission

- Protects everywhere — from remote laptops to JWCC enterprise clouds.



Zscaler & Glasswall Integration – Solution Brief

Secure IL5-to-IL6 Data Transfer – Zscaler Private Access (ZPA) & Glasswall

Zscaler Private Access (ZPA) delivers Zero Trust access for IL5 systems, encrypting, segmenting, and policy-enforcing at every step. Glasswall disarms every file crossing the boundary.

Key Benefits

- ✓ Enhanced Security: Zscaler and Glasswall combine to protect data integrity and remove threats across IL5 and IL6.
- ✓ Compliance: Meets DOD IL5 and IL6 requirements, including air-gapped SIPRNet environments.
- ✓ Operational Efficiency: Enables secure, seamless data sharing for mission-critical operations and mission partners.
- ✓ Scalability: Leverages Zscaler's cloud-native architecture and Glasswall's orchestration for enterprise-grade scalability.

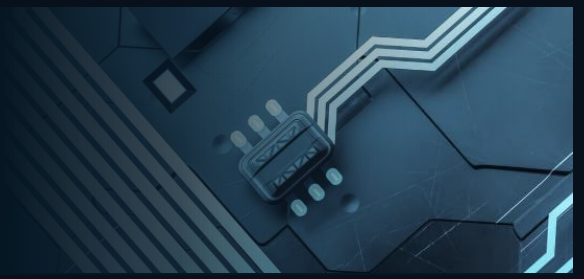
Proven in Mission-Critical Environments

GLASSWALL + EVERFOX

Trusted Gateway System (TGS)

Secure Multi-Directional File Transfer for Segmented Networks

Website



GLASSWALL + BAE SYSTEMS

XTS® Guard 7

XTS Enterprise Guard is the key component to secure information sharing within government agencies, military frameworks, and Intelligence agencies.

Website

GLASSWALL + ARCFIELD™

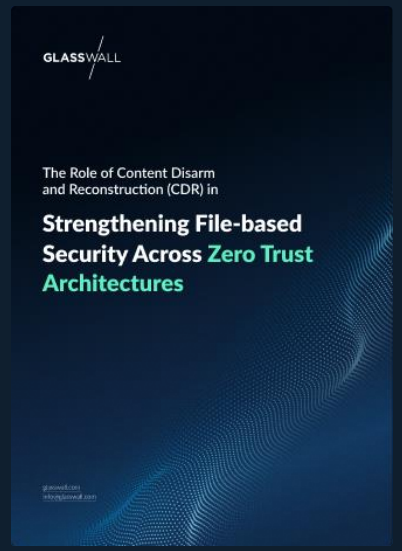
X-ARBITOR

Enables U.S. government agencies and coalition partners operating at different classification levels to share information

Website

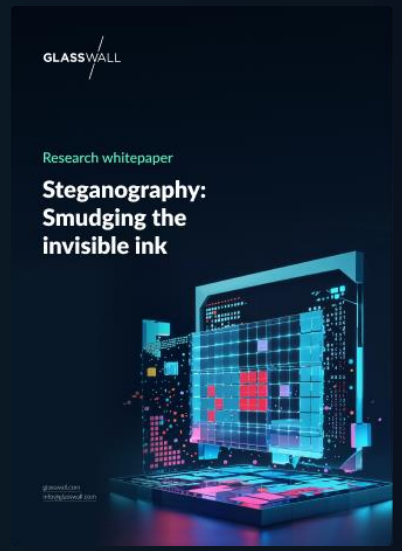
Glasswall's Partner Ecosystem

Want To Go Deeper?



Zero Trust Whitepaper
https://www.glasswall.com/resource/zerotrust-whitepaper

Polyglot Research Whitepaper
https://docs.glasswall.com/docs/polyglot-research-unmasking-images-pdf



Steganography Mitigation Whitepaper
https://docs.glasswall.com/docs/steganography-smudging-the-invisible-ink

QR Code Whitepaper
https://docs.glasswall.com/docs/qr-codes-neutralizing-threats-with-cdr-detection-and-removal

Talk to us

to strengthen your file security

Chris Wyman

DOD Sales Director
cwyman@glasswall.com
571-217-0910

Kelly Davis

Sr. Solution Architect
kdavis@glasswall.com
973-930-1983

GLASSWALL

Try it today at halo.glasswall.com