GLASSWALL

The Role of Content Disarm and Reconstruction (CDR) in

Strengthening File-based Security Across Zero Trust Architectures

glasswall.com
info@glasswall.com

Executive Summary

The U.S. Department of Defense (DoD) and other mission-critical organizations **struggle to protect against a growing wave of file-based attacks.** **Zero trust** has become the **foundation of modern cyber-security**, but without robust file sanitization, warfighters and enterprises alike face critical blind spots. Content Disarm and Reconstruction (CDR) addresses this gap by ensuring only clean, fully functional files enter an organization's environment – **eliminating threats before they pose a risk to mission success.**

The 'zero trust' security model, and it is based on the premise that, by default, nothing interacting with IT infrastructure is trusted, regardless of whether it's inside or outside a network. As such, it has become one of the security industry's most important approaches to addressing the rising levels of breaches.

The challenge is that file-based threats remain a significant blind spot, as traditional security methods – such as antivirus, sandboxing, and AI-based detection – struggle to effectively mitigate malware infiltration, hidden exploits, and advanced persistent threats (APTs) within Zero Trust Architectures (ZTAs).

This whitepaper examines how Content Disarm and Reconstruction (CDR) bridges this security gap by proactively eliminating file-based threats to ensure only clean, fully functional files enter an organization's ecosystem. Unlike detection-based approaches, which attempt to identify malicious content, CDR assumes all files are untrusted and rebuilds them to a "known good" state, fully aligning with zero trust principles. This paper also draws on insights from high-stakes environments like the DoD, where tactical edge operations demand secure data access in Denied, Degraded, Intermittent, and Limited (DDIL) scenarios.

This paper explores:

Introduction

The zero trust model has become a cornerstone of modern cybersecurity, transforming how mission-critical organizations protect their networks, devices, and data in contested environments. From the U.S Department of Defense (DoD) to commercial enterprises, Zero Trust Architectures (ZTAs) enforce continuous verification, eliminate implicit trust and provide a strong defense against unauthorized access and lateral movement. However, while identity, network segmentation, and endpoint security are often the focus of zero trust strategies, one of the most exploited attack vectors remains largely unaddressed: file-based threats.

Cybercriminals have adapted to zero-trust environments by embedding malware, ransomware, and other exploits within common file formats such as PDFs, Office documents, and email attachments. Traditional detection-based security measures – including antivirus, sandboxing, and AI-driven analysis – are often ineffective against these threats due to their reliance on known signatures and behavioral patterns. This leaves organizations exposed to sophisticated attacks that can bypass traditional defenses and compromise sensitive data.

To mitigate this risk, organizations must rethink how they secure files within a zero trust framework, especially in areas where connectivity is unreliable. Content Disarm and Reconstruction (CDR) offers a proactive, prevention-first approach by assuming all files are untrusted. Instead of scanning for threats, CDR rebuilds files from the ground up, removing potentially malicious elements while preserving full functionality. This paper explains how.

GLASSWALL

Section 1

The Role & Importance of Zero Trust Architectures

As cybercrime costs race toward $23 trillion by 2027, the “never trust, always verify” mindset has become the cornerstone of modern security. From Forrester’s early insights to federal mandates, zero trust is redefining how we defend networks and data.

Organizations in every sector face the **growing risks of criminal and nation-state attacks** on their networks and data. The annual average cost of **cybercrime** is predicted to hit more than $23 trillion in 2027, up from $8.4 trillion in 2022, according to data from the U.S. Deputy National Security Advisor.

(Source: The Economist)

As a result, there is growing momentum behind the "never trust, always verify" approach to cybersecurity.

This is the 'zero trust' security model, and it is based on the premise that, by default, nothing interacting with IT infrastructure is trusted, regardless of whether it's inside or outside a network. The phrase was first coined by Forrester Research in 2010 and has become one of the security industry's most important approaches to addressing the rising levels of security breaches.

> *A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). Access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established.*
>
> National Institute of Standards and Technology NIST

US Government Zero Trust Mandate

The value of zero trust has been recognized at the highest levels. The U.S. government's Zero Trust mandate, outlined in Executive Order 14028, requires federal agencies to implement a security model that eliminates implicit trust and enforces continuous verification of users, devices, and network activity. This approach strengthens cybersecurity by mandating multi-factor authentication, least privilege access, micro-segmentation, and real-time threat detection to protect critical systems and data, ensuring force protection across the enterprise and tactical edge.

Zero Trust Supports the Mission

The U.S. military's latest zero trust initiatives, including the Department of the Navy Chief Information Officer (DON CIO) Zero Trust Blueprint and the Army Unified Network Plan (AUNP) 2.0, underline the shared commitment to securing networks and data in an increasingly contested global landscape.

The Army Unified Network Plan (AUNP) 2.0:

Zero Trust forms the foundation of the Army's cybersecurity strategy, guided by eight principles, including "never trust, always verify," "presume breach," and "least privilege." They focus on securing data at every echelon, preventing unauthorized access, and modernizing encryption to safeguard data integrity.

The Army's AUNP 2.0 expands on its original framework to deliver a secure, data-centric architecture based on zero trust, supporting multi-domain operations even in disconnected or degraded environments. Centralising service delivery and focusing on secure data sharing, the plan integrates hybrid cloud, AI/ML, and interoperability with mission partners while progressing toward future capabilities like quantum-resistant encryption.

The Navy DON CIO Zero Trust Blueprint:

The Navy's Zero Trust Blueprint provides a comprehensive framework for securing all operational layers, involving users, devices, applications, data, and networks. It sets out a strategic shift toward full zero trust alignment by FY2030, addressing the complexity of modern cyber threats through layered security, micro-segmentation, AI-driven threat detection and strict access controls.

Framing cybersecurity as a "cyber chess match," the strategy emphasizes real-time resilience in contested environments, end-to-end data protection, and workforce development. They operate under the assumption that adversaries may possess superior visibility, employ deception, and disregard conventional rules.

The Navy also adheres to stringent standards, such as NIST 800-207 for and NIST 800-53 for security controls, while collaborating with enterprise ICAM services and Cyber Security Service Providers (CSSPs) to integrate best-in-class solutions.

GLASSWALL

Section 2

ZTA Security Vulnerabilities

Zero trust is powerful, but it's not invincible. Attackers can still slip through via stolen credentials, supply chain breaches, or malicious files.

Zero Trust Architectures (ZTAs) aim to eliminate implicit trust within networks and, when implemented correctly, are extremely effective in protecting mission-critical operations. However, they also introduce significant security **challenges that organizations, including those at the tactical edge, need to understand and address.**

These include:

1. Implementation complexity

Deploying zero trust can require significant architectural changes. Misconfigurations and integration issues can create security gaps, leading to unintended vulnerabilities.

2. User & device verification gaps

Weak authentication mechanisms, stolen credentials, or session hijacking can allow attackers to bypass zero trust controls and gain unauthorized access.

3. Supply chain vulnerabilities

Attackers often target third-party vendors and service providers to infiltrate organizations, bypassing zero trust protections through compromised external partners.

4. Credential and token theft

Cybercriminals exploit authentication weaknesses using phishing, API abuse, and token theft to gain unauthorized access to sensitive data.

5. Lateral movement risks

While zero trust restricts movement within networks, poor segmentation or misconfigurations may still allow attackers to navigate internally after an initial breach.

6. Overhead & performance issues

Continuous authentication and verification processes may introduce latency and impact system performance, requiring careful optimization.

7. Ineffective cyber hygiene

Human errors, misconfigured policies, and outdated access controls can weaken the effectiveness of a zero trust strategy, leading to potential security lapses.

8. Integration challenges

Legacy systems may lack support for modern authentication methods, making it difficult to enforce zero trust principles across an entire organization.

9. Cloud data security

With sensitive data spread across multiple cloud providers, improper access controls, weak encryption, or misconfigured cloud environments can lead to breaches. The Army's hybrid cloud strategy and Unified Data Reference Architecture (UDRA), as outlined in the AUNP 2.0 highlights the need for robust cloud security to prevent breaches

10. Attacker evasion techniques

Threat actors continuously adapt their tactics to bypass zero trust controls, including embedding malicious payloads in files or exploiting zero-day vulnerabilities, a concern in the Navy's "cyber chess match" environment where adversaries focus on deception to evade detection.

11. File-based vulnerabilities

Malicious files, including PDFs, Office documents, and email attachments, are an increasingly common and effective attack vector. Without protection from robust file sanitization measures such as Content Disarm and Reconstruction (CDR), attackers can exploit vulnerabilities in file formats to deliver malware, bypassing traditional security controls.

12. Disconnected environments

In disconnected environments, like Denied, Degraded, Intermittent, and Limited (DDIL) scenarios highlighted in the AUNP 2.0, continuous verification becomes difficult due to unreliable connectivity. The AUNP 2.0 emphasizes this challenge where soldiers at forward operating bases must access data securely despite unreliable connectivity.

GLASSWALL

Section 3

Understanding File-based Security risks in a Zero Trust Context

Malicious files hide in plain sight—1 in every 100,000 can be weaponized, and most slip past antivirus tools for weeks. Attackers exploit these gaps for ransomware, espionage, and data theft. A zero trust mindset, bolstered by proactive defenses like Content Disarm and Reconstruction, least-privilege access, and continuous monitoring, is vital to keep files secure.

File-based cyber threats remain a persistent challenge for organizations, especially as digital workflows rely heavily on file exchanges across networks and cloud platforms. With one in every 100,000 files containing potentially malicious content, attackers continue to exploit security gaps to infiltrate organizations.

Traditional detection-based security, such as antivirus and sandboxing, falls short against these evolving threats, exposing businesses to Advanced Persistent Threats (APTs), ransomware gangs, and cybercriminals who leverage file security weaknesses to execute sophisticated attacks.

Evolving Threat Actor Tactics

Even with Zero Trust Architecture (ZTA) eliminating implicit trust, adversaries continuously adapt their tactics to exploit file security weaknesses. APTs, often backed by nation-states, use malicious files in supply chain attacks, compromising trusted software updates or vendor communications to embed backdoors into enterprise systems.

Ransomware gangs, emboldened by growing profits from extortion schemes, are also focusing on file-based attacks. Attackers frequently use malicious file downloads, phishing emails, and cloud-based collaboration platforms to deliver ransomware payloads. Once activated, these attacks encrypt critical data, disrupt operations, and often employ double extortion tactics, where attackers steal sensitive information before encrypting it, threatening to leak data unless ransoms are paid. Beyond ransomware, threat actors exploit file-based vulnerabilities for espionage, financial gain and to cause disruption.

Credential-harvesting attacks use weaponized file attachments to deploy keyloggers or steal login credentials, granting unauthorized access to sensitive networks. Attackers also use malicious files to exfiltrate intellectual property or disrupt operations through denial-of-service attacks. Cloud storage and collaboration tools are also targeted because perimeter-based security approaches are no longer sufficient to contain these risks

A Zero Trust Approach to File Security

A zero trust approach to file security requires organizations to eliminate implicit trust in files and enforce strict security controls. Instead of relying on traditional detection-based security – which struggles against emerging threats – businesses must adopt proactive solutions such as Content Disarm and Reconstruction (CDR). This technology neutralizes hidden threats by rebuilding files to their "known good" state before delivery, removing embedded malware while ensuring usability.

Implementing least-privilege access controls limits the potential damage of a file-based attack, ensuring that even if a malicious file enters the network, its impact is contained. Continuous monitoring and behavioral analytics help detect anomalies in file activity, flagging suspicious behaviors before they escalate. Additionally, multi-factor authentication (MFA) and strong identity verification further protect against unauthorized access, ensuring that even if attackers compromise a file, they cannot easily execute it within the organization's environment.

GLASSWALL

Section 4

The Role of CDR in Strengthening File-based Security Across ZTAs

Content Disarm and Reconstruction (CDR) is zero trust's secret weapon against file-based threats. By rebuilding files to a safe "known good" state—without slowing down workflows—CDR thwarts hidden malware, supports compliance, and delivers instant, threat-free access to critical data.

Content Disarm and Reconstruction (CDR) is a proactive cybersecurity technology that eliminates file-based threats by treating all incoming files as untrusted, closely aligning with the requirements of a zero trust architecture. Unlike traditional security solutions that rely on detecting known threats, CDR deconstructs files to their core components, removes potentially harmful elements, and rebuilds them to a clean and safe version that adheres to manufacturer standards. This ensures files are threat-free while maintaining their original usability and functionality.

CDR Use Cases

CDR is being applied across a wide range of mission-critical zero trust use cases in government and commercial organizations. The technology is well suited to business documents and media files where file specifications are well established, ensuring that known good is well understood.

Cross Domain Solutions (CDS)

CDR eliminates reliance on detection-based security and data wrapping commonly used to protect cross-domain environments. Its zero trust approach assumes all files are potentially malicious – validating, rebuilding, and delivering only known-good content. The most effective CDR solutions also support compliance with key industry best practices and security frameworks, including guidelines from national cybersecurity agencies & regulatory bodies, such as the National Institute of Standards and Technology (NIST).

File Upload Portals

Organizations and government entities frequently ingest files from external sources, but traditional approaches can expose them to risks from embedded threats. Integrating zero-trust file sanitization capabilities at multiple points within an organization's security architecture enables the automatic removal of both known and unknown file-based threats. This ensures that only secure, visually identical, and fully functional files reach end users.

Cloud Migration

Transferring files across trust boundaries – within internal infrastructure or between public and private networks – poses a security challenge, especially during cloud migrations. Organizations can leverage scalable CDR solutions via REST-based integrations to process large storage repositories at high speed, ensuring that only safe, clean, and fully functional files move across networks.

Web Appliances

Implementing real-time file sanitization within network security infrastructure – such as proxy servers, firewalls, and gatewats – enhances threat mitigation. By integrating CDR capabilities via ICAP servers, organizations can actively remove embedded threats from web traffic, ensuring safe content delivery.

Post-Breach Remediation

With the rise of sophisticated cyber threats, including nation-state attacks and AI-generated malware, effective post-breach recovery is more critical than ever. CDR technology offers an advanced zero-trust approach to neutralizing threats within files, making it a key component in post-breach remediation strategies for mitigating malware and ransomware risks.

Advantages of CDR

For organizations adopting a zero trust approach, CDR delivers a variety of important advantages, adding a robust layer of protection against file-based security threats:

- **Zero trust protection**

  Assumes all files are untrusted, neutralizing both known and unknown threats (zero-day vulnerabilities).

- **No reliance on detection**

  Traditional antivirus and sandboxing solutions depend on identifying malicious signatures, leaving gaps for novel threats. CDR removes all risks upfront.

- **Seamless user experience**

  Unlike sandboxing, which delays access, CDR delivers files instantly, maintaining productivity.

- **Automated security**

  CDR removes threats without manual intervention, reducing security team workload and improving operational efficiency.

- **Compliance and standardization** – ensures all files conform to industry standards, supporting regulatory compliance and reducing security blind spots.

CDR vs Other File Security Methods

In addressing file-based security risks, organizations have a range of technology options. A major challenge is that traditional detection-based methods, such as antivirus and sandboxing, struggle to keep pace with evolving threats, making CDR a proactive alternative that eliminates hidden risks rather than simply identifying them. Here's how the different approaches compare:

Technology	Zero-Day Malware Protection	File Handling	Update Requirements
CDR	Removes unknown threats by design	Files are secured instantly with usability maintained	Doesn't require an internet connection or updates
Antivirus	Relies on signature-based detection, ineffective against novel threats	Files are held or quarantined	Requires constant database updates
Sandboxing	Sandbox-aware malware can bypass detection	Files are held or quarantined	Needs updating to protect against the newest threats
EDR	Can be evaded by targeted malware that falsifies information	Files are held or quarantined	Needs updating to protect against the newest threats
File Flattening	Removes active content but does not neutralize zero-day exploits	Files are turned into images at the cost of functionality, making usable edits impossible	Often legacy systems require updating

GLASSWALL

Section 5

How to Select a CDR solution

Not all CDR solutions are created equal.
The most effective maintain full file functionality, use trusted libraries for safe rebuilding, provide in-depth threat reporting, scale to handle large data loads, and show proven success with government or defense agencies.

> *CDR is an important layer in any organization's defense and content protection strategies.*
>
> Gartner®

There are a number of CDR solutions on the market, but not all are created equal, and organizations should evaluate solutions based on some key selection criteria:

1. Are all file types fully functional once they have been processed?

When choosing a CDR vendor, it is important to investigate which solutions process file types in their intended format and which don't. There are a number of technologies on the market that lack the capability to process a wide range of file types in their intended format. To overcome this and to provide support for as many file types as possible, files are transformed into a simple flat file type, such as a JPEG image file, allowing for it to be processed by the vendor's CDR technology and made safe.

However, the process of file flattening strips the file of its original functionality, in many cases removes its usability altogether. This reduces a user's ability to work collaboratively on a document, disrupting their workflow & reducing workplace productivity.

In addition, many CDR vendors have an extensive list of supported file types, and while that may be impressive at first glance, a closer inspection often finds that few are processed in their intended file type. This isn't always clear from a vendor's market-facing content, so when reviewing vendor options, it's important to ensure that a distinction is made between which files their technology truly 'CDRs' and which file types are flattened to enable processing to take place.

2. Does the vendor use manufacturer-recommended libraries to reconstruct a file?

File rebuilding is an integral part of why CDR is considered the best defence against file-based threats. This stage of the CDR process uses libraries to rebuild a file back to a secure standard.

However, when selecting a CDR vendor, it is important to consider which libraries are used to rebuild files.

It is common for CDR vendors to utilize non-proprietary libraries to rebuild files. While this removes malicious content hidden within the original file structure, these can still leave vulnerabilities hidden within the processed document structure – leaving the organization at risk even when a file has been processed.

3. Can the vendor report on all non-conforming parts of a file?

Many CDR vendors lack the capability to provide granular reporting on the threats found while processing a file. Without this information, security teams cannot collect intelligence about the risks facing their organization, leading to information fragmentation and, ultimately, blind spots in their wider cyber defenses.

Some regulations also require organizations to report on the mitigating actions they have taken to remove the risk cyber threats pose to them – without granular reporting. This can become a headache for security teams because they have to reprocess an original file to understand the risks included within it.

4. Can the vendor handle large-scale data processing?

Whether organizations are processing a number of files from a local device or large storage containers before or during a data migration, it is important to consider if the CDR vendor can process data at the scale required. While most CDR vendors emphasize scalability to some degree, the key differentiator within the marketplace is performance while processing at scale. To impact business-as-usual operations as little as possible, the chosen CDR solution's performance should be maintained across large-scale projects.

5. Has the solution been tested and validated by government/ defense organizations?

CDR vendors should be able to demonstrate a proven track record working with government and defence agencies and commercial organizations in regulated sectors and should be willing to share evidence of their success. Steer clear of organizations that claim their capabilities and successes but are unwilling to provide supporting evidence.

6. Which CDR classification level does the vendor offer?

Content Disarm and Reconstruction (CDR) solutions are classified into levels based on their capabilities, as outlined in the Industry Framework for Content Disarm and Reconstruction. Glasswall CDR is classified as a Level 3 Advanced CDR, the highest classification, which signifies its ability to perform deep file inspection, reconstruction, and sanitization while preserving full functionality and ensuring compliance with stringent standards. Unlike Level 1 (basic stripping of active content) or Level 2 (partial reconstruction) solutions, Glasswall deconstructs files to their core components, validates them against manufacturer specifications, remove all non-conforming elements, and rebuilding them into a fully functional, threat-free version.

The advanced Level 3 CDR capability is critical for Zero Trust Architectures, as it ensures no malicious content, known or unknown can infiltrate an organization's ecosystem, even in high stake and highly contested classified environments where zero day exploits are a constant threat. The Level 3 classification also supports compliance with standards like NIST 800-207, making it an ideal solution for organizations and government agencies requiring the highest level of file based security.

Level 1 - CDR

Flattens and converts the original file to a PDF

Level 2 - CDR

Strips out active content while keeping the original file type

Level 3 - Advanced CDR

Eliminates all file-borne risk while maintaining file type

GLASSWALL

Section 6

How Does Glasswall CDR Support the Zero Trust Model?

Zero Trust means never assuming files are safe. Glasswall takes this principle to heart by instantly stripping out hidden threats and rebuilding each file to its 'known good' standard—no waiting, no guesswork. Unlike other CDR tools, Glasswall preserves full functionality while delivering truly threat-free files, closing critical security gaps and keeping workflows seamless.

Content Disarm and Reconstruction (CDR) is a proactive cybersecurity technology that eliminates file-based threats by treating all incoming files as untrusted, closely aligning with the requirements of a zero trust architecture. Unlike traditional security solutions that rely on detecting known threats, CDR deconstructs files to their core components, removes potentially harmful elements, and rebuilds them to a clean and safe version that adheres to manufacturer standards. This ensures files are threat-free while maintaining their original usability and functionality.

Glasswall CDR plays a critical role in helping government organizations meet the file security demands outlined in zero trust strategies from across the U.S. Department of Defense:

The Army Unified Network Plan (AUNP) 2.0:

For the Army, Glasswall CDR can facilitate secure data sharing through the MPE, ensuring every file exchanged with allies is free of threats, even in DDIL conditions or when using cross-domain solutions (CDS) for secure transfers. Additionally, our technology secures Office 365 applications by ensuring that every Word document, Excel spreadsheet, or other file is safe, mitigating a key risk area for the Army's Zero Trust integration.

The Navy DON CIO Zero Trust Blueprint:

For the Navy, Glasswall CDR can secure data at every Policy Enforcement Point (PEP), aligning with their micro-segmentation and continuous monitoring objectives. Their reliance on User and Entity Behavior Analytics (UEBA) as a "lynchpin" for threat detection can be enhanced by the ability to provide clean data for analysis, and generating reports to improve threat detection accuracy, which could directly support the Navy's analytics efforts.

Detection-based security methods – such as antivirus and sandboxing solutions – have to play catch up with new and unknown threats and malware that contain malicious code. Adding a CDR capability to the cybersecurity stack is vital in a rounded zero trust cybersecurity strategy, particularly in the fight against malicious file uploads.

As recently highlighted by Gartner, organizations are advised to: "Restrict the file types to the minimum required. For allowed file types, there are essentially four options to limit the risk of malware upload: CDR provides the highest security. Done well, CDR removes all threats from uploaded files without adding significant latency. Since it does not depend on detecting known threats, it can even protect against completely new attack types."

A trusted four-step protection process

Glasswall CDR technology instantly removes risk by using a patented process:

Step 1
Inspect

Three file layers are inspected to validate that its digital DNA complies with the 'known good' manufacturer's specification. Remediation instantly takes place where deviations are found.

Step 2
Rebuild

The file is rebuilt to its known good manufacturer's standard, ensuring it is clean and threat-free. Structural malformations (whether benign or malign) are repaired, with alien objects being ejected from the file to defeat even the most sophisticated attacker. Glasswall's deep understanding of file formats ensures that the rebuilt file contains only safe structures beneath the visual layer.

Step 3
Clean

High-risk active content within the visual layer (i.e. macros and embedded links) is cleaned and removed based on content policy – so only the users who need active content receive it.

Step 4
Deliver

The user instantly receives a safe, identical file that's compliant, standardized and trusted – reducing the risk of the malicious code hidden in malware while maintaining business continuity. The result is a powerful ability to close the security blindspots exploited by cybercriminals who know that reactive antivirus and sandboxing technologies cannot identify new vulnerabilities hidden in file 'DNA' for days or even weeks after they have been released. Unlike other CDR solutions that flatten files or rely on outdated reconstruction methods, Glasswall ensures files retain their full functionality while removing risks at a forensic level.

GLASSWALL

Section 7

Glasswall CDR solutions

From embedded engines to turnkey deployments, Glasswall's advanced CDR suite delivers flexible, zero trust file protection for any environment—even offline. Trusted by top intelligence agencies, it neutralizes hidden threats while preserving full file functionality, ensuring robust security without disrupting workflows.

Glasswall offers industry-leading CDR solutions that provide flexible and scalable protection against file-based threats:

Glasswall Embedded Engine

Seamless integration of industry-leading CDR protection

The Glasswall Embedded Engine is designed for organizations seeking to enhance their cyber-security posture. Delivered as a software development kit (SDK) with an application programming interface (API), it enables fast and effective integration into new and existing applications to eliminate file-based threats. The Embedded Engine supports Linux & Windows operating systems and can be deployed in a containerized form, ensuring high portability and ease of deployment across diverse IT environments.

Glasswall Halo

Scalable, out-of-the box zero trust file security

Glasswall Halo is an award-winning, out-of-the-box, zero-trust CDR file protection designed for scalable deployment. Built on a Kubernetes-based architecture, it dynamically adjusts to meet organizational needs - whether protecting a small volume of files or processing large-scale document flows. Glasswall Halo is a turnkey solution enabling security teams to quickly and efficiently safe-guard their organization from file-based threats. Its deployment is streamlined through Helm Charts, facilitating rapid implementation and easy upgrades to maintain optimal security performance.

Glasswall Meteor

Zero-trust file protection for isolated environments

Glasswall Meteor enhances security by providing automated, zero-trust file protection with advanced file synchronization and drag-and-drop processing capabilities. Designed to function even in offline environments, Meteor is ideal for organizations operating in air-gapped systems, remote locations, and other isolated environments where continuous network connectivity is not guaranteed.

Trusted by the world's leading intelligence agencies and organizations

Glasswall's CDR platform has been tested, validated and implemented by a range of the world's leading intelligence agencies, who have successfully protected against all efforts to penetrate the technology even when custom-written exploits have been used to test the product. The analytics and policy management output and level of security delivered by Glasswall have always exceeded expectations - no other CDR technology has undergone such extensive, independent testing.

Further reading:

AWS - 'Embracing Zero Trust: A strategy for secure and agile business transformation'

Navy DON CIO Zero Trust Blueprint (2025)

Army Unified Network Plan (AUNP) 2.0 (2025)

NIST Special Publication 800-207: Zero Trust Architecture

Take the next step in securing your zero trust strategy

Request a demo today to address the vulnerabilities leaving your network exposed.

Book a demo

glasswall.com
info@glasswall.com