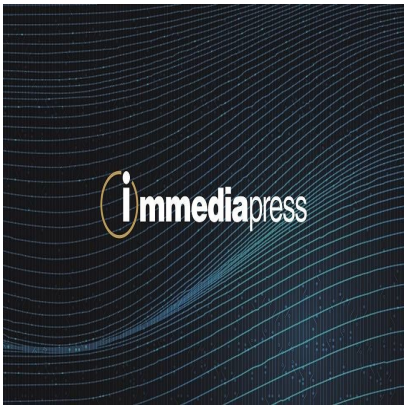

Glasswall Introduces a New Class of File-Based Threat Intelligence with the Launch of Foresight

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

New AI-powered Threat Prediction Gives Security Teams Visibility Into Unknown and Zero-Day File Threats

WASHINGTON, March 10, 2026 /PRNewswire/ â?? Glasswall, an industry-leading provider of intelligent Zero Trust file protection solutions in both the business-to-government (B2G) and business-to-business (B2B) sectors, has today announced the launch of Glasswall Foresight, a new AI-powered solution that applies machine learning with deep Content Disarm and Reconstruction (CDR) analysis deliver predictive insight into file-based threats, helping organizations identify and stop new and unknown malware, including zero-day attacks.

Unlike behavioral sandboxing or internet-trained AI models that rely on detonation or external threat feeds, Foresight derives its intelligence directly from deterministic file structure analysis generated during Glasswallâ??s CDR process.

Now available in Glasswall Meteor, Glasswallâ??s automated file cleaning application for local and cloud storage, Foresight enhances endpoint security with a new level of intelligent protection. By combining machine learning with Glasswallâ??s proven CDR technology, the solution provides visibility into the malicious nature of files, including those that have been safely processed or cannot be modified. This enables security teams to better understand the level of file-based threat activity in their environments. In practice, this allows security teams to prioritize high-risk files, enrich investigations with contextual threat scoring, refine Zero Trust policies, and surface structured risk data directly into SIEM and SOC workflows.

By analyzing hundreds of thousands of potential indicators drawn from millions of samples, Foresight generates a probabilistic classification that reflects the likelihood of a file being malicious, including

previously unseen or zero-day threats. This intelligence enables organizations to better understand the threat landscape within their file-based workflows, even in environments where traditional detection technologies fall short.

Glasswall Foresight is designed to complement, not replace, existing CDR workflows, extending Glasswallâ??s Zero Trust approach from file sanitization into actionable threat intelligence. Built on trusted CDR telemetry rather than generic AI models, the solution operates effectively in offline and air-gapped environments and provides security teams with reliable insight, supported by production-grade models delivering an extremely low false positive rate of 0.015 percent for PDFs (with similarly low rates across common enterprise formats including DOCX and XLSX), which helps reduce analyst fatigue and SOC workload.

By integrating directly into Glasswall Meteor, Foresight enables organizations to better understand file-based threat activity while maintaining the preventive, policy-driven controls central to Glasswallâ??s file security methodology.

â??File-based threats remain one of the most effective and persistent attack vectors facing public and private sector organizations, yet traditional threat intelligence and detection tools struggle to keep pace with unknown and zero-day attacks,â?• said Paul Farrington, Chief Product and Marketing Officer at Glasswall.

â??With Glasswall Foresight, we are applying machine learning to the deep structural insight generated by our Content Disarm and Reconstruction technology to give security teams a clearer understanding of the hostile file activity entering their environments, including in offline or air-gapped conditions where conventional approaches fall short. Combining the assurance that we make a file safe with the knowledge of whether it has ever been compromised is compelling. Many organizations invest heavily in sandboxing infrastructure that is slow, noisy, and expensive. Glasswallâ??s Zero Trust CDR combined with Foresight provides a clear path to reducing both that expenditure and the associated operational overhead.â?•

For further information, visit: www.glasswall.com

About Glasswall

Glasswall is a cybersecurity company that protects government agencies and commercial organizations from malicious files with its Content Disarm and Reconstruction (CDR) technology. Unlike traditional detection-based methods, Glasswall employs a Zero Trust approach that removes malwareâ??s ability to exist in files altogether. An acknowledged file protection innovator, the company is investing heavily in research and development to deliver new approaches to understanding, predicting, and mitigating file-based threats. Glasswallâ??s CDR technology is mandated for use as a file filter in Cross Domain Solutions by the NSA and is trusted by the worldâ??s most sophisticated security establishments.

To learn more about Glasswall, visit www.glasswall.com.

Photo â?? https://mma.prnewswire.com/media/2928302/Glasswall.jpgLogo
â?? https://mma.prnewswire.com/media/2839627/5840475/Glasswall_Logo.jpg

View original content to download multimedia:https://www.prnewswire.co.uk/news-releases/glasswall-introduces-a-new-class-of-file-based-threat-intelligence-with-the-launch-of-foresight-302708574.html

â??

immediapress/pr-newswire

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Marzo 10, 2026
Autore
redazione