

AI Resilience for the Post-Mythos Era.

A lightweight, rapid-response offering to counter the speed of AI-powered exploitation.

Deployed in days, not months.

- CONTINUOUS
- AUTONOMOUS
- VENDOR-AGNOSTIC



/// THE MOMENT

The math of vuln management just *changed*.

Anthropic's Project Mythos has uncovered thousands of high-severity vulnerabilities across every major OS and browser. AI-generated exploits now emerge within hours of disclosure; meanwhile, the average organization still measures patching in weeks or months.

Manual triage, ad-hoc ticketing, and CVE-by-CVE remediation were built for a slower world. They do not survive this volume.

/// ANTHROPIC GUIDANCE

"Patch internet-facing assets within 24 hours and prepare for 10x the volume of critical CVEs."

1000s

High-Severity Vulns

Found across every major OS and browser

10x

Expected CVE Volume

Manual triage won't survive this volume

24hrs

Max Patch Window

Anthropic's recommended window for internet-facing assets

/// INTRODUCING ZAFRAN AIR

Build AI resilience now.

Zafran AIR is a rapid-response offering designed to help organizations stand up AI resilience immediately. Continuous detection, deployed in days, with fast-track pricing, so your team can focus on closing exposure gaps instead of navigating procurement cycles.

/// DEPLOY IN DAYS, NOT MONTHS

Agentless, API-based. Layers on top of your existing security stack. No rip-and-replace.

/// VENDOR-AGNOSTIC SOLUTION

Integrates across your existing tools so you can act on risk in one place, not locked into a single vendor.

/// CUT TIME TO NEUTRALIZE FROM DAYS TO MINUTES

Autonomous agents detect exploitability, prioritize what matters, and route remediation in minutes.

/// WHAT'S INCLUDED

Designed for *Rapid Response*.

Zafran AIR gives you everything you need to build AI resilience in a post-Mythos era: faster detection, exploitability assessment, autonomous agents, plus a Mythos-tuned dashboard and the KPIs your board will ask about.

Zero-Day Agent

- ✓ Detects exploitability within 24 hours of disclosure and automatically routes response to the right owners minutes after detection.

Unified, continuous vulnerability detection

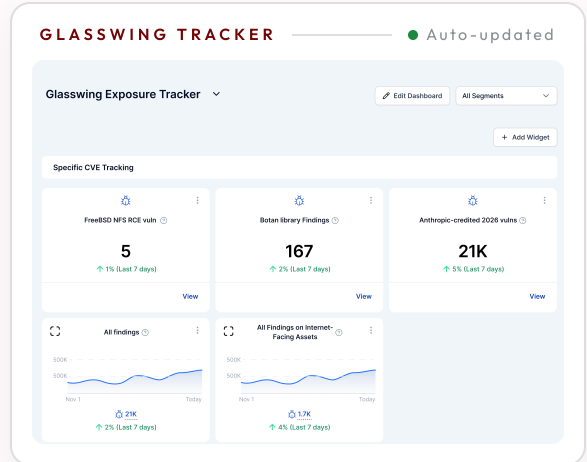
- ✓ Unify cloud and on-prem findings from your existing scanners, with continuous SBOM detection ahead of CVE enumeration. No new agents.

Autonomous exploitability assessment

- ✓ Internet exposure, runtime presence, and live threat intel (KEV · EPSS · exploit-in-the-wild) to automate triage and focus on the real risk.

Project Glasswing Exposure Tracker

- ✓ A purpose-built dashboard for Mythos-class disclosures. Updates the moment a new vulnerability exposure is detected.



A Mythos-tuned dashboard. Track remediation velocity across your fleet from disclosure through fix.

The *Zero-Day Agent*.

The Zero-Day Agent continuously runs across your existing stack, answering the question every team asks when a new zero-day drops: *am I exposed?* It detects exploitability within 24 hours of disclosure and automatically routes response to the right owners minutes after detection.

