InvisRisk Expands Build Application Firewall with Real-Time CI/CD Enforcement Across AWS and GitLab

New release extends runtime policy enforcement, stopping software supply chain threats during build execution before release.

HOUSTON, TX, UNITED STATES, June 29, 2026 /EINPresswire.com/ -- InvisiRisk today announced a major step forward in securing modern software delivery pipelines, advancing its Build Application Firewall (BAF) to deliver real-time enforcement during CI/CD execution — an approach that addresses a critical gap left by traditional security tools — to AWS CodeBuild and GitLab CI/CD.

As software supply chain attacks increasingly target the build process itself, most security solutions still rely on scanning code before or after execution. This model fails to detect or stop malicious behavior that executes during the build, where compromised dependencies, scripts, or pipeline actions can access sensitive data and perform unauthorized actions.

InvisiRisk's Build Application Firewall takes a fundamentally different approach. Instead of scanning artifacts in isolation, the platform enforces what a build is allowed to do while it is running—monitoring behavior and stopping policy violations and zero-day attacks in real time.

"Security tools today are built around the assumption that if code looks safe before or after execution, it is safe to run," said Eric Pulaski, CEO of InvisiRisk. "That assumption is no longer valid. Attacks are increasingly activating inside the build process itself. InvisiRisk was built to enforce security at that exact moment, when it matters most."

With the latest release, version 1.1.41, InvisiRisk extends real-time enforcement across two additional CI/CD environments: AWS CodeBuild and GitLab CI/CD. Organizations can now apply Build Application Firewall policies consistently across pipelines and automatically stop builds at the point of violation—directly within the runner—before insecure code progresses further downstream.

The release also introduces a new InvisiRisk BAF Check Summary within GitHub Actions, giving developers immediate visibility into risk and policy violations within their existing workflows. By surfacing enforcement results where builds occur, InvisiRisk integrates security directly into the development process rather than requiring separate analysis tools.

These capabilities reinforce a shift from passive detection to active control in software supply chain security:

- From scanning to enforcement: Security policies are applied and enforced during build execution, not just analyzed before or after
- From alerts to action: Builds are automatically stopped when violations occur
- From visibility gaps to runtime control: Behavior inside the build process is monitored and governed in real time

InvisiRisk's approach addresses a growing class of attacks that evade traditional tools by executing during CI/CD runs, including malicious dependencies, compromised build scripts, and credential exfiltration attempts. By enforcing policies during execution, organizations can prevent these attacks before code is packaged or released.

The release also simplifies deployment through a unified setup process, reducing the complexity of integrating real-time enforcement into existing CI/CD workflows.

InvisiRisk's Build Application Firewall was introduced to protect the most vulnerable stage of modern software delivery—the build pipeline itself. This latest release strengthens that vision by expanding enforcement coverage and embedding security directly into developer workflows.

"As attacks move into the build pipeline, security has to move there too," Pulaski added. "This is not about better scanning. It's about controlling what your build is allowed to do in real time."

About InvisiRisk

InvisiRisk released the industry's first Build Application Firewall (BAF) in 2025, the first security platform purpose-built to protect CI/CD pipelines at the network level during the build process itself. Using deep packet inspection technology, InvisiRisk enforces what a build is allowed to do in real time, stopping credential theft, supply-chain tampering, and unauthorized exfiltration before compromised code ever reaches production.

Eric Pulaski
InvisiRisk
+1 713-627-3800
press@invisirisk.com

---

in today's world. Please see our Editorial Guidelines for more information.