InvisiRisk Expands Build Application Firewall with Encoded Secret Detection and Hardened CI/CD Integration

Latest release (v1.1.38) delivers real-time encoded secret interception, deep dependency intelligence, and expanded GitHub Actions support

HOUSTON, TX, UNITED STATES, April 22, 2026 /EINPresswire.com/ -- InvisiRisk, which released the industry's first Build Application Firewall (BAF) in 2025, today announced a major platform update that strengthens real-time protection of CI/CD pipelines against encoded credential exfiltration, supply-chain compromise, and dependency manipulation techniques driving today's most damaging attacks.

The release comes amid a sharp rise in software supply-chain attacks targeting trusted build, package, and CI/CD workflows. Recent campaigns, including TeamPCP and Shai-Hulud, have shown how attackers can compromise the software delivery process itself to steal credentials, tamper with dependencies, and push malicious code downstream. Yet most security tools still focus on code at rest, cloud posture, or deployed workloads, leaving the live build process with limited runtime protection.

InvisiRisk's Build Application Firewall is the industry's only solution designed for deep packet inspection of build traffic during CI/CD pipeline execution. Where traditional tools scan before or after the build, InvisiRisk enforces what a build is allowed to do in real time, detecting and blocking exfiltration, unauthorized network calls, and malicious dependency behavior as it happens.

"Build systems and CI/CD pipelines have become one of the most active fronts in software supply-chain attacks, and the pace and sophistication of those attacks has accelerated in 2026," said Eric Pulaski, CEO of InvisiRisk. "Major attacks this year have shown that scanning code at rest or monitoring infrastructure after deployment misses the moment that matters most. Our deep packet inspection technology was built to enforce security while the pipeline is running, where attackers are increasingly operating. This release extends that protection and gives teams better visibility into build-time activity and the complex chain of transitive dependencies behind modern applications."

What's New in v1.1.38

Encoded Secret Interception at Build Time
• Real-time detection and blocking of encoded secrets during active builds, including Base64, double-Base64, and layered encoding schemes observed in recent Sandworm-style campaigns.
• Deep inspection of outbound request bodies and headers as builds execute, not limited to source code scans or post-build artifact analysis.
• Prevents credential exfiltration even when hidden inside approved API calls, allow-listed destinations, or encrypted traffic.

Full Dependency Graph and Supply-Chain Intelligence
• New interactive dependency graph maps the complete chain of direct, transitive, and cached dependencies consumed during each build, providing an accurate software bill of materials (TruSBOMTM).
• Expanded package ecosystem coverage across RubyGems, Debian, Alpine, and cached dependency layers to reflect how modern builds actually resolve and fetch packages.
• Improved ecosystem-specific vulnerability attribution ensures accurate risk mapping across dependency paths.

Hardened GitHub Actions Integration
• Extended automatic BAF integration for GitHub Actions now supports Docker-based builds alongside standard workflows, closing a critical coverage gap.
• Improved reliability with pre-run validation checks, multi-account handling, and build lifecycle notifications.
• Supports both GitHub App-based automation and YAML-driven configurations for easier deployment across team structures.

AI-Assisted Policy Engine and Signal Refinement
• AI-assisted policy generation with configurable enforcement modes (warn or deny) lets security teams define and enforce build-time controls without slowing developer velocity.
• Streamlined policy assignment with enforced unique naming reduces configuration drift and operator error.
• Refined anomaly detection engine reduces false positives while preserving high-signal event fidelity.

Built for Today's CI/CD Attack Patterns
Recent attacks have made clear that software supply-chain risk increasingly extends into the live build process. Attackers are not limited to planting backdoors in source code; they are abusing package resolution, release automation, and pipeline execution to steal credentials, manipulate dependencies, and move downstream through trusted delivery paths.

Most existing approaches — including cloud-native application protection platforms (CNAPPs), static application security testing (SAST), and software composition analysis (SCA) tools, were not designed to observe or enforce policy on live build traffic as a pipeline runs. InvisiRisk's Build Application Firewall closes that gap by inspecting and enforcing build-time network behavior in

real time, across every CI/CD run.

When a compromised dependency, a malicious post-install script, or a supply-chain worm attempts to exfiltrate a secret from inside a build, InvisiRisk can detect and block the attempt before that activity becomes downstream damage.

Availability
All enhancements in v1.1.38 are available immediately to InvisiRisk customers. To learn more or request a demo, visit invisirisk.com.

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
press@invisirisk.com
