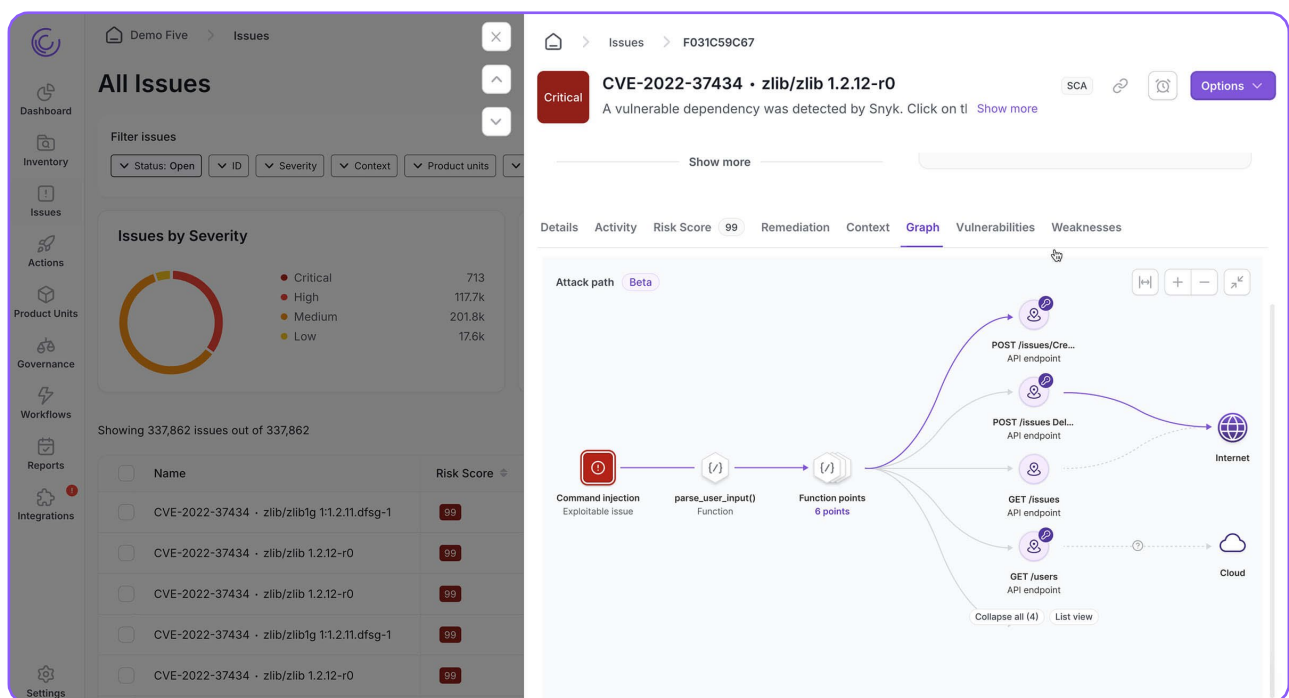


Legit Security is frequently a reference point for enterprises looking for an application security posture management tool. They were the first to make me aware of the ASPM category, and when I saw the product, the solution immediately made sense for those dealing with the “too many scanners” problem. Development teams at large enterprises frequently manage their own pipelines and tools, leading to sprawling and uncertain scanning coverage. Legit steps in to provide teams with a strong mapping of their deployment pipelines, cloud-based or on-premise, and assigns risk and coverage scores as code moves through to deployment.

Within the last few years, Legit has expanded well beyond providing a pure management layer. The platform now includes scanning capabilities like SAST and SCA, API reachability, and significant change tracking. For management and consolidation use cases, these additions have meaningfully increased the overall value of the solution.



With the recent launch of VibeGuard, Legit Security is on the front lines of addressing challenges with AI code generation. VibeGuard covers critical capabilities, starting with securing AI code generation tools - IDE's, MCPs, and rules - preventing attacks like prompt injection and unapproved secret access. It then helps to secure code as it's generated by fetching organizational and security context, allowing teams to enforce security standards on AI generated code.

Together, these capabilities form a holistic, modern platform that is particularly well suited for enterprise environments.

The Benefits of Legit Security

Gain Visibility Across Deployment Pipelines

Track and monitor workflows to maintain oversight across dispersed development teams, gaining a complete coverage map of your SDLC.

Enforce Governance for AI-Generated Code

Embed AI Governance into development flows, securing end to end developer usage from code generation to ensure secure MCP usage.

Track Changes Across Enterprise Environments

Teams can assess overall coverage and security posture across their tooling, while using Legit to close gaps across traditional scanners and emerging AI-driven coding workflows.