



DATASHEET

# Legit ASPM for AI-Driven Software Development

AI is revolutionizing how software gets built – faster, smarter, and more autonomous. But it's also rewriting the rules of application security. Traditional AppSec tools weren't designed for AI-driven dev processes or code written by AI.

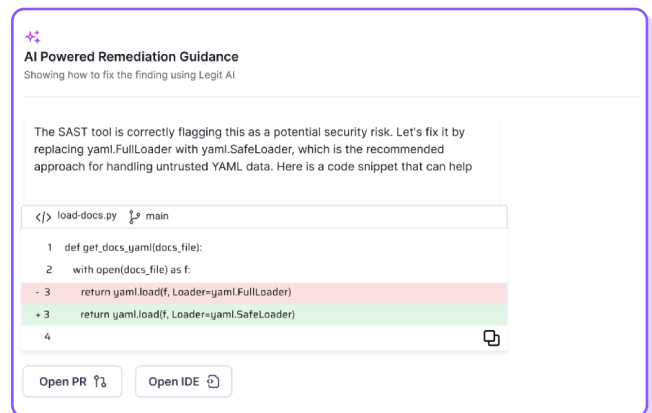
Legit ASPM is the first and only AI-native ASPM platform purpose-built to secure today's development workflows, including those with AI at the core.

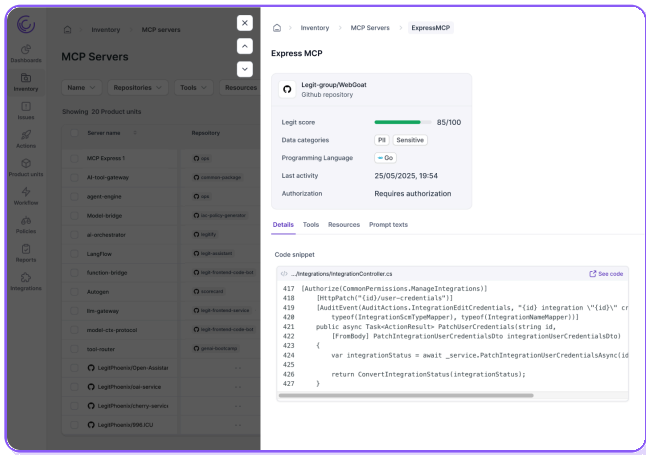
We at Legit are both helping our customers use GenAI securely, and leveraging it ourselves to expand the capabilities of our AI-native ASPM platform.

Here's how ↓

## AI Remediation

With Legit's AI-based remediation, security and development teams both go to one system to get the clarity and guidance they need to remediate the right security issues quickly. Legit adds contextual AI-based remediation code snippets to SAST and SCA findings, making the how and why behind the fix crystal clear. Teams can also open PRs directly within Legit.



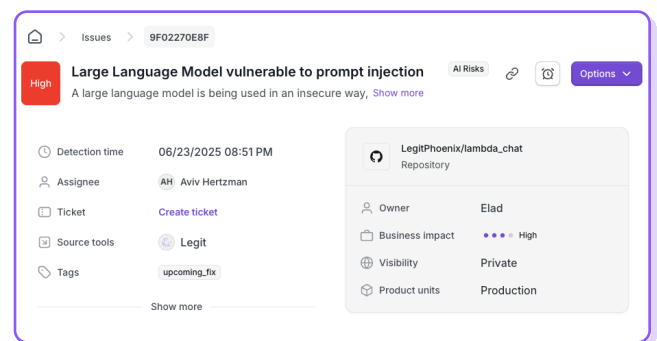


## AI Discovery

AI use in development is a black hole for most AppSec teams. It's hidden across code and pipelines, risking drift, unapproved use, and policy violations. Acting as your complete AI governance solution, Legit scans code, pipelines, and repos to provide full discovery and monitoring of all AI off-the-shelf models and in-house MCPs.

## AI SAST

AI vulnerabilities like prompt injection, insecure model use, and missing validation are not identified by traditional SAST tools. Legit AI SAST detects AI-specific code security issues with tailored rules that understand AI patterns.



## AI Code Assistant Integration

Legit gives developers real-time security insights and remediation embedded directly into their AI-powered assistants — no learning curve, no context switching, all in natural language.

Through our MCP Server, AI code assistants like Cursor, GitHub Copilot, and Windsurf leverage Legit to determine the security of code produced, enforce guardrails to prevent issues, and drive automated remediation.

## AI Agents for ASPM

Legit's AI Agents empower you to automate all three phases of ASPM: complete context, prioritization and remediation, along with "Ask AI" automating the ability to identify app owners, triage, set up workflows, generate reports, remediate, and get next-steps guidance.



Trace pulls together data points from code to cloud to create the data fabric Legit uses to map pipelines and risk.



With the insights of the Trace Context Agent, Serenity makes it easy to understand what must be fixed based on risk.



After Trace and Serenity have done their jobs, Healy gets to work making automated fixes and offering recommendations to developers.



Astro lives within the Legit platform and makes it easy for users to search, create reports and take actions using clear, natural language.

## Learn More About Legit Security

[Visit Our Website](#)

### About Legit Security

The Legit Security ASPM platform is a new way to manage application security in a world of AI-first development, providing a cleaner way to manage and scale AppSec and address risks. Fast to implement, easy to use, and AI-native, Legit has an unmatched ability to discover and visualize the entire software factory attack surface, including a prioritized view of AppSec data from siloed scanning tools. As a result, organizations have the visibility, context, and automation they need to quickly find, fix, and prevent the application risk that matters most. Spend less time chasing low-risk findings, more time innovating.