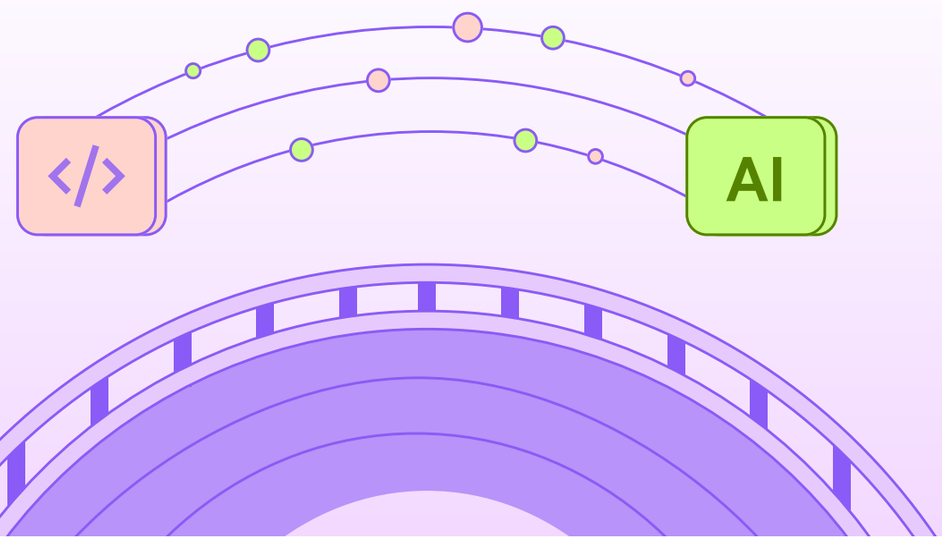
LEGIT

Legit MCP Server



Legit's Model Context Protocol Server adds trust and security to AI-led coding

Tomorrow's Secure Coding, Today

With Legit's Model Context Protocol (MCP) Server, AI tools and code assistants leverage Legit to determine the security of code produced, flag vulnerabilities, enforce guardrails to prevent issues, and drive automated remediation.

Bringing ASPM to AI-led development, the Legit MCP Server makes vulnerability management as simple as asking a question. This, in turn, reduces the risk of disruption from human-based errors or security checks, automates the developer experience, and increases agility for fast development and deployment.

Legit MCP is full-context security intelligence that lives inside your team's workflows, so security becomes part of the conversation - not an interruption.

Use Cases

Legit MCP Server addresses a comprehensive and broad range of software development and security needs:

Developer use cases:

- Integrate Legit's MCP server to all popular IDEs and code assistants (Cursor, Copilot, Windsurf, Claude Code, and more)
- Ensure secure vibe coding when using AI-assisted development
- Get real-time detection of and remediation guidance for security findings directly within AI code assistants

Security teams use cases:

- Rapid security posture insights and report creation, directly via AI assistants like Claude and ChatGPT
- Alerts and detailed analyses of emerging risks and trends relevant to your organization's technology stack

Automate Secure Coding

MCP lets developers take ownership of security, right inside code assistant tools like Cursor, Copilot, Windsurf, and Claude Code. Ask a security question, and Legit MCP responds with contextual answers pulled from your actual codebase and security posture data. With this real-time visibility and validation of AI-generated code, developers ensure any legacy libraries or insecure code is detected at the build phase.

Get Real-Time Contextual Security

With Legit MCP, you reduce the security team workload by asking Claude Desktop questions like:

- "Show me vulnerability reduction trends in internet-facing apps this month"
- "What's the current security posture of our customer database application?"
- "Which teams introduced the most critical issues last quarter?"

Legit MCP answers in seconds with unified, organization-wide insights that help the team test and discover in-code vulnerabilities, weaknesses, and misconfigurations.

Embed Trust and Reduce Disruption

Legit MCP fetches data from every connected AppSec tool and source, delivering one consistent, trustworthy view across your entire SDLC.

You get a single source of security truth—accessible through natural language.

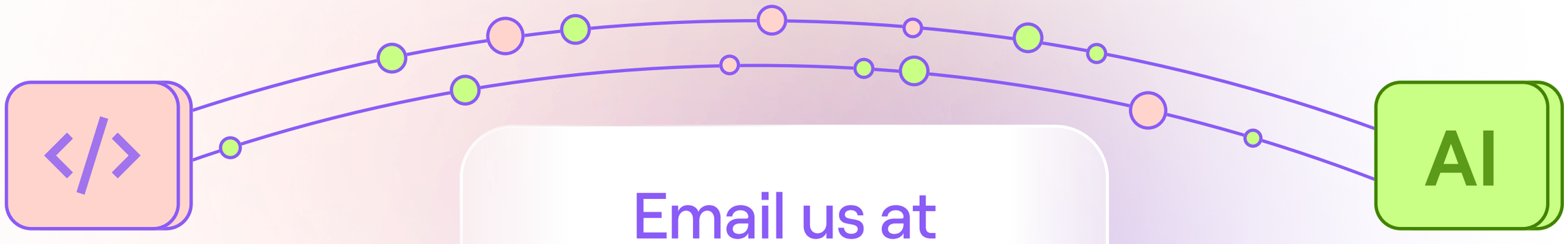
Integration With IDEs

Claude · Windsurf · GitHub Copilot · CURSOR · Cline

Legit ASPM Platform

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.



Email us at

info@legitsecurity.com