

Sparrow MCP

AI-Powered Security Assistant for Safe AI-Driven Software Development

AI is Redefining Software Development

AI coding assistants and agents such as Claude Code and Cursor are becoming an integral part of modern software development, accelerating code generation, modification, testing, and delivery.

Security Must Move Into the AI Loop

AI-generated code is created and modified continuously, making traditional post-development security validation insufficient.

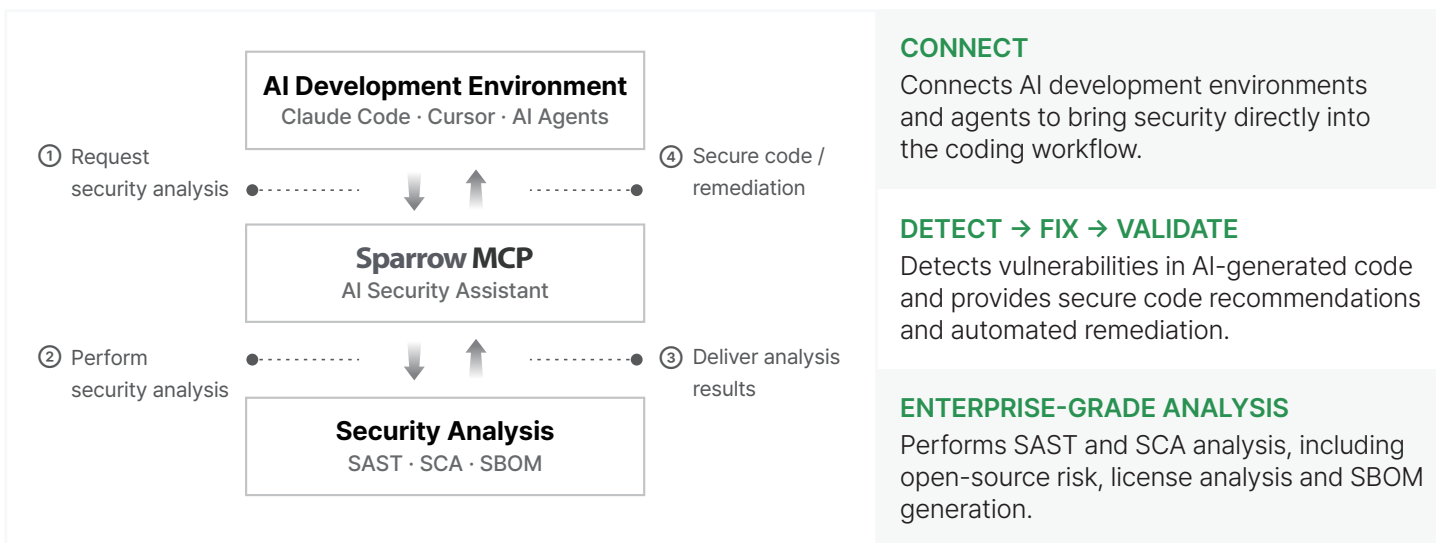
- Security feedback must be available inside the AI coding workflow
- AI development can bypass existing security checkpoints
- Security must operate at the same speed as AI-driven development

New AI Development Risks

- Prompt Injection & Malicious Instructions
- Vulnerable AI-generated Code
- Sensitive Data Exposure
- Unsafe Agent & Tool Actions
- Open-source & Software Supply Chain Risks

What is Sparrow MCP ?

Secure AI-generated code as it is created
— with real-time SAST, SCA and automated remediation.



Key Features

- AI-generated Code Security Analysis
- Real-time SAST & SCA
- Open-source Risk & License Analysis
- AI-powered Secure Code Recommendations
- Automated Vulnerability Remediation
- Continuous Security Validation

Business Value

- Secure AI Development at Scale
- Reduce AI-generated Code Risks
- Accelerate Secure Software Delivery
- Strengthen Software Supply Chain Security
- Enterprise Governance for AI-driven Development