Trust Agent: AI

Secure and scale AI-driven development

AI is writing code. Who's governing it?

The challenge: AI-assisted coding risks

The widespread adoption of AI coding tools presents a critical new challenge: a lack of visibility and governance over AI-generated code. While these tools improve developer productivity, they simultaneously introduce significant security risks to your organization.

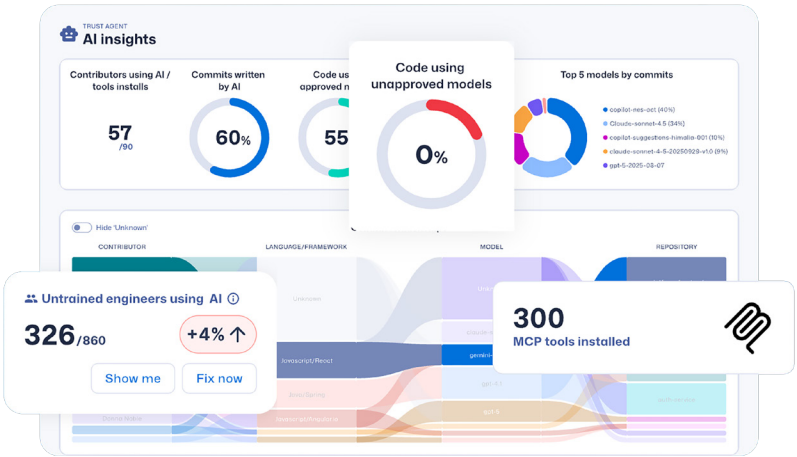
- **78%** of developers are currently utilizing AI tools in their development processes.
- However, up to **50%** of AI-generated code contains security weaknesses, spanning across **38** different vulnerability categories.

Without a dedicated way to manage AI usage, CISOs and engineering leaders are exposed to questions they cannot answer. Organizations face a lack of visibility into which developers are using unapproved models, uncertainty around the security proficiency of those developers, and an inability to enforce policy and governance.

The solution

Meet the AI Software Governance Platform: the control plane for AI-driven software risk across your Software Development Life Cycle (SDLC).

SCW empowers organizations to embrace the speed of AI-driven development without sacrificing security by providing real-time visibility and governance for both human and AI-generated code.



Developers currently utilizing AI tools in their development processes

78%

AI-generated code containing security weaknesses, spanning across **38** different vulnerability categories

50%

Ready to govern the future of code?

Gain visibility into your AI-driven development lifecycle today.

Visibility, governance, and measurable impact

How it works: Trust Agent: AI

The new AI capabilities of SCW Trust Agent provide the deep observability and control you need to confidently manage AI adoption. Trust Agent delivers actionable insights in three key steps:

- **Detects and analyzes AI-assisted coding activity:** Deployed as an IDE plugin or endpoint agent, it observes AI-assisted coding activity gene generated by tools like GitHub Copilot, ChatGPT, Google Gemini, and Cursor in real-time.
- **Enriches data with skill levels:** It correlates this AI usage data with the contributing developer's verified secure coding proficiency.
- **Enforces proactive governance:** Security teams can identify unsanctioned LLM use, spot developers with limited security knowledge committing AI code, and define and evolve governance policies and guardrails to improve the overall security posture.

SUPPORTED IDE & AGENT ENVIRONMENTS:

Cline
KIRO
ROOCODE
aider
GitHub Copilot
Claude
Gemini
CURSOR
Windsurf
openCode

SUPPORTED LLM APIS:

GitHub Copilot
Amazon Bedrock
Vertex AI
OpenAI
Gemini
OpenRouter
ANTHROP\C

Upskill your team in the era of AI

SCW supports enterprises transitioning to AI-assisted development by addressing the critical skills gap.

- **Comprehensive learning:** Access over **700+** AI and LLM interactive learning activities — including AI Challenges, Coding Labs, and Quests — that simulate pull requests and teach developers to critically validate AI suggestions.
- **Broad coverage:** Training covers over **75** coding languages and **650+** real-world vulnerabilities.
- **AI Security rules:** Utilize free, lightweight guardrails to help tools like Copilot and Cursor generate safer code by default.

The SCW advantage

By integrating SCW into the tools your developers use daily, you can maximize release velocity, reduce the rework required for security bugs, ship secure code with confidence, and ultimately protect your brand's reputation and sensitive data.

About Secure Code Warrior

Secure Code Warrior is a leader in AI software governance and developer security upskilling, enabling enterprises to control AI-driven software development across the SDLC. Built on a decade as the leading secure coding training platform, it brings together AI visibility, governance, and hands-on learning to prevent vulnerabilities and improve software quality before production.

Ready to govern the future of code?
Gain visibility into your AI-driven development lifecycle today.

SEE **TRUST AGENT: AI IN ACTION.**