SECURE CODE WARRIOR

AI insights
AI code in critical repositories
75%
+5%
Code written by AI
40%
Commits using AI
63%
Commits with unapproved models
29%
Untrained engineers leveraging AI
326/860
Top providers by usage

SCW Trust Agent: AI

Visibility and Governance to Secure AI-Assisted Development

As developers rapidly adopt AI coding tools, CISOs, AppSec, and engineering leaders face a critical new challenge: a lack of visibility and governance over AI-generated code. This challenge is already felt today, with Stack Overflow's most recent annual survey finding that over 78% of developers are using AI coding tools in their development process.

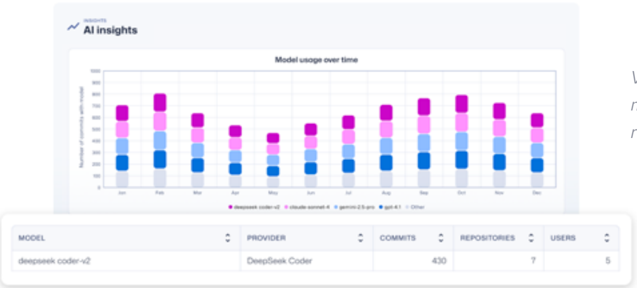
Secure Code Warrior firmly believes security-proficient developers using the right LLMs will build code much faster with less security technical debt. However, the opposite is true as well. Because LLM-powered code assistants often produce insecure code, we know that developers must still possess fundamental knowledge of secure coding to identify and remediate vulnerabilities produced by AI-tooling.

Any gaps can lead to significant risk when AI-generated code is committed without sufficient oversight or developer secure coding proficiency. Organizations need a way to confidently embrace AI-driven development without sacrificing security.

What is SCW Trust Agent: AI?

SCW Trust Agent: AI is a new set of capabilities that provide deep observability and governance over AI coding tools, LLM and MCP usage within the software development lifecycle (SDLC). Trust Agent: AI uniquely correlates three key signals– a developer's AI coding tool usage, their code contributions, and their secure coding skill level—to provide unparalleled insights into AI-assisted developer risk at the commit level. Security and engineering leaders can now proactively manage the impact of AI-assisted code generation across their application development landscape and answer questions they previously could not, including:

- *Who is using code generating AI tools and on which code repositories?*
- *Are my development teams using company approved LLMs?*
- *What MCPs are being used?*
- *What percentage of contributed code was written by an LLM?*



MODEL	PROVIDER	COMMITS	REPOSITORIES	USERS
deepseek coder-v2	DeepSeek Coder	430	7	5

View commits by model, publisher, code repository and more

With Trust Agent: AI, security and engineering leaders gain the confidence and control to integrate AI coding tools in their development teams' arsenals without compromising their organization's security posture.

Values and Benefits

Observability

Gain deep visibility into AI-assisted software development, including which developers are using which LLMs and MCPs and on which code repositories.

Governance

Automate policy enforcement to ensure AI-enabled developers meet secure coding standards before their contributions are accepted.

Optimize the Development Lifecycle

Address security challenges around AI-assisted development early to reduce vulnerability backlogs, accelerate development, and mitigate risk.

Risk Metrics

Connect AI-generated code to actual commits to understand the true security risk being introduced.

50%

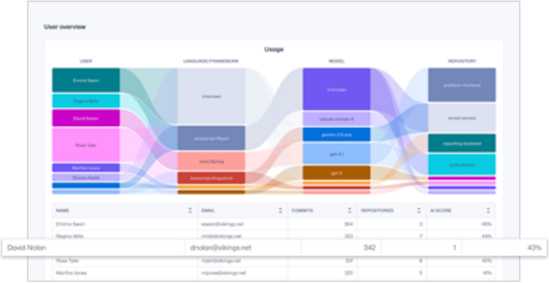
of functionally correct LLM-produced code is insecure -BaxBench

30%

of AI-generated code contains security weaknesses, related to 38 different CWE categories -arXiv

Powered by SCW Trust Agent

Powering new AI capabilities is SCW Trust Agent, an industry-first offering that closes the gap between LLM-generated code contributions and developer secure coding proficiency. Trust Agent: AI gives you the complete visibility and control required to manage AI-assisted developer risk at its source- the actual code commit.

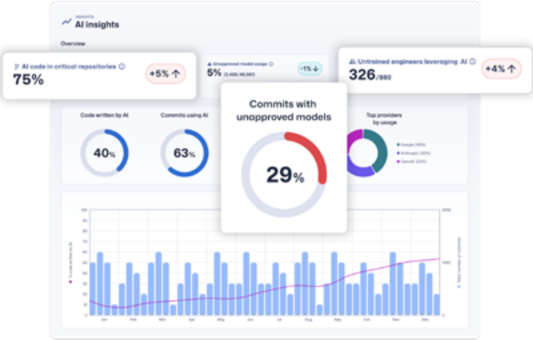


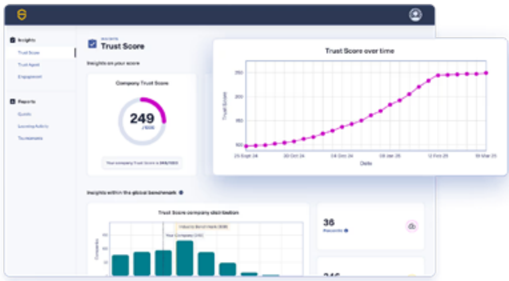
Actionable Insights

Get detailed views into specific code commits, AI/LLM-tooling used, and the contributing developer's secure coding proficiency. Dashboards provide actionable insights including unsanctioned LLM use and identification of developers with limited secure coding knowledge who are committing AI-generated code.

Integrated Governance with Commit Controls

Trust Agent: AI offers integrated governance at scale through flexible policy gating controls. Define policies based on a project's sensitivity and compliance requirements, proactively applying secure coding standards and AI policy directly at the commit level. If a developer attempts to commit code generated by an unapproved model, or they lack secure coding proficiency, Trust Agent: AI can be configured to automatically log, warn, or even block a pull request.





Secure Code Warrior Learning

SCW Learning is the engine behind developer security competency, providing the essential skills needed to safely leverage AI-assisted coding. The product includes **SCW Trust Score,** an industry-first benchmark that quantifies developer security proficiency across organizations. **AI Challenges,** a brand-new Copilot-style experience, and over 200+ AI/LLM/MCP learning activities equip developers to identify and remediate security vulnerabilities in AI-generated code

Extensive Code Repository Support

Deploy Trust Agent in any Git-based source code management tool, including GitHub, GitLab, Bitbucket, Azure Repos, and more.

GitHub GitLab

ATLASSIAN Bitbucket Azure Repos

About Secure Code Warrior

Secure Code Warrior is a Developer Risk Management Platform enabling enterprises to measure, manage and mitigate risk. Improve security posture and reduce vulnerabilities by up to 53% with our integrated approach of organizationally benchmarking developer secure code skills, governance through quality gates integrated during code changes and upskilling with a dynamic on-demand secure code learning platform. Trusted by over 600 enterprises to help them deliver secure software rapidly and create a culture of developer-driven security.

securecodewarrior.com | **Request a demo** |

SECURE CODE WARRIOR