# Secure Code Warrior unveils Trust Agent: AI for enhanced security governance amid rising AI-driven code risks



Secure Code Warrior has launched a beta programme for expanded AI capabilities within its Trust Agent product, aimed at giving chief information security officers (CISOs) enhanced traceability, visibility, and governance over how developers use AI coding tools. This upgrade, branded Trust Agent: AI, integrates multiple data signals—from AI coding tool usage and vulnerabilities to code commit activity and developer secure coding skills—to provide security leaders with a comprehensive understanding of the risks introduced by artificial intelligence during the software development lifecycle.

The introduction of large language models (LLMs) has revolutionised code generation speed, yet it has also raised significant security concerns. Current industry tools often fail to monitor which AI coding solutions developers use or how much code AI generates unchecked, leaving unknown vulnerabilities and potential biases embedded in software. Secure Code Warrior co-founder and CEO Pieter Danhieux emphasised this risk, stating that "using the wrong LLM by a security-unaware developer, the 10x increase in code velocity will introduce 10x the amount of vulnerabilities and technical debt." He highlighted how Trust Agent: AI aims to fill this gap by providing the data needed to filter security-proficient developers for sensitive projects while monitoring and managing the AI tools used throughout the day.

Trust Agent: AI is notable as the first solution designed to map the dynamic relationship between developers, the AI models they employ—including vulnerabilities those models might introduce—and the repositories where AI-produced code is committed. This capability enables enterprises to trace generative AI usage across extensive codebases and link it directly to security outcomes. Such detailed monitoring is crucial as organisations adopt AI-driven development practices at scale but seek to manage emerging risks effectively.

The product introduces integrated governance and observability features spanning multiple development stages. Key functions include detecting unapproved LLMs and exposing associated vulnerabilities, enforcing flexible policy controls to log, warn, or block pull requests from developers using unsanctioned tools or lacking secure coding skills, and analysing the proportion and location of AI-generated code across repositories. These policy controls empower security teams to align developer capacities with organisational security mandates while maintaining oversight of the accelerated code production enabled by AI.

Secure Code Warrior’s Trust Agent platform already supports various Git-based source control systems such as GitHub, GitLab, and Bitbucket, offering deep insights into developer risk by analysing every code commit for security competencies tailored to multiple languages and frameworks. It seamlessly integrates with the company’s Agile Learning Platform to address gaps in skills, ultimately fostering a security-first development culture and helping reduce vulnerabilities in code bases. Trust Agent also contributes to achieving compliance and improving productivity by embedding security practices directly into developer workflows.

While the full general release of Trust Agent: AI is scheduled for 2026, Secure Code Warrior has opened an early access programme for organisations keen to participate in the beta phase. The company positions this product as a key enabler for enterprises to recalibrate their security programmes amid the increasing embedment of generative AI tools in software development. By delivering advanced analytics and governance capabilities, Trust Agent: AI is intended to support CISOs in making informed, data-driven decisions regarding AI deployment, responding proactively to new risks emerging from high-velocity AI code generation.

Secure Code Warrior’s broader commitment remains focused on reducing breach risks by building security-awareness among developers. Their platform provides extensive hands-on learning opportunities across more than 60 languages and frameworks with over 8,000 learning activities, supporting organisations in nurturing secure coding expertise and establishing resilient, Secure-by-Design development practices.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://securitybrief.com.au/story/secure-code-warrior-debuts-trust-agent-ai-for-code-risk-insight), [[4]](https://www.securecodewarrior.com/solutions/mitigate-risk)
* Paragraph 2 – [[1]](https://securitybrief.com.au/story/secure-code-warrior-debuts-trust-agent-ai-for-code-risk-insight)
* Paragraph 3 – [[1]](https://securitybrief.com.au/story/secure-code-warrior-debuts-trust-agent-ai-for-code-risk-insight)
* Paragraph 4 – [[1]](https://securitybrief.com.au/story/secure-code-warrior-debuts-trust-agent-ai-for-code-risk-insight), [[2]](https://www.securecodewarrior.com/product/trust-agent), [[3]](https://www.securecodewarrior.com/press-releases/secure-code-warrior-introduces-industry-first-solution-that-measures-developers-security-competencies-for-code-commits), [[6]](https://www.securecodewarrior.com/press-releases/secure-code-warrior-introduces-industry-first-solution-that-measures-developers-security-competencies-for-code-commits)
* Paragraph 5 – [[2]](https://www.securecodewarrior.com/product/trust-agent), [[3]](https://www.securecodewarrior.com/press-releases/secure-code-warrior-introduces-industry-first-solution-that-measures-developers-security-competencies-for-code-commits), [[4]](https://www.securecodewarrior.com/solutions/mitigate-risk), [[7]](https://www.securecodewarrior.com/solutions/mitigate-risk)
* Paragraph 6 – [[1]](https://securitybrief.com.au/story/secure-code-warrior-debuts-trust-agent-ai-for-code-risk-insight)
* Paragraph 7 – [[4]](https://www.securecodewarrior.com/solutions/mitigate-risk), [[7]](https://www.securecodewarrior.com/solutions/mitigate-risk)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://securitybrief.com.au/story/secure-code-warrior-debuts-trust-agent-ai-for-code-risk-insight> - Please view link - unable to able to access data
2. <https://www.securecodewarrior.com/product/trust-agent> - Secure Code Warrior's Trust Agent provides visibility and control to scale developer-driven security. It analyses every commit against developer secure code skills, offering insights into code repositories and aligning security competencies with code commits. The platform aims to mitigate risks, increase productivity, and achieve compliance by embedding security practices into the development process. Trust Agent supports various Git-based source code management tools, including GitHub, GitLab, and Bitbucket, and integrates with the SCW Agile Learning Platform to enhance developer security knowledge.
3. <https://www.securecodewarrior.com/press-releases/secure-code-warrior-introduces-industry-first-solution-that-measures-developers-security-competencies-for-code-commits> - Secure Code Warrior has introduced SCW Trust Agent, an industry-first solution that assesses developers' security competencies for every code commit. This tool enables security leaders to gain deeper visibility into their organisations' software development security posture, facilitating a Secure-by-Design approach. Trust Agent works seamlessly with Git-based code repositories, including GitHub, GitLab, and Bitbucket, and allows administrators to set up policies ensuring developers meet baseline standards before developing code. It also integrates with the SCW Agile Learning Platform to address any gaps in developer skills.
4. <https://www.securecodewarrior.com/solutions/mitigate-risk> - Secure Code Warrior focuses on reducing the risk of breaches by building a team of security-aware developers. Their platform enhances team expertise, fosters a security-centric culture, and helps organisations establish a security-first approach to prevent vulnerabilities in code bases. The platform offers over 60 languages and frameworks, hands-on learning, and more than 8,000 learning activities. It also provides SCW Trust Agent, which analyses developer secure code competencies on a per-language basis for every commit in repositories, offering actionable insights and customizable policy controls.
5. <https://www.securecodewarrior.com/products/developer-risk-management> - Secure Code Warrior offers developer risk management solutions, including the SCW Trust Score, which quantifies the impact of secure coding initiatives. The SCW Trust Score provides a comprehensive assessment of an organisation's secure coding skills, enabling AppSec teams and CISOs to understand their team's competencies and identify areas for optimisation. The platform also offers observability and governance for risk management through SCW Trust Agent, providing visibility into developers' security skills and allowing policy configuration for code repositories to improve security posture.
6. <https://www.securecodewarrior.com/press-releases/secure-code-warrior-introduces-industry-first-solution-that-measures-developers-security-competencies-for-code-commits> - Secure Code Warrior has introduced SCW Trust Agent, an industry-first solution that assesses developers' security competencies for every code commit. This tool enables security leaders to gain deeper visibility into their organisations' software development security posture, facilitating a Secure-by-Design approach. Trust Agent works seamlessly with Git-based code repositories, including GitHub, GitLab, and Bitbucket, and allows administrators to set up policies ensuring developers meet baseline standards before developing code. It also integrates with the SCW Agile Learning Platform to address any gaps in developer skills.
7. <https://www.securecodewarrior.com/solutions/mitigate-risk> - Secure Code Warrior focuses on reducing the risk of breaches by building a team of security-aware developers. Their platform enhances team expertise, fosters a security-centric culture, and helps organisations establish a security-first approach to prevent vulnerabilities in code bases. The platform offers over 60 languages and frameworks, hands-on learning, and more than 8,000 learning activities. It also provides SCW Trust Agent, which analyses developer secure code competencies on a per-language basis for every commit in repositories, offering actionable insights and customizable policy controls.