

AI CODING ASSISTANTS

IN FOCUS: GitHub Copilot, a language-agnostic coding tool that makes real-time suggestions inside the developer's coding environment.

Beyond the hype and hysteria, AI-powered coding assistants show real potential to support enterprise software development. To get the most out of these tools, you need to understand risks and mitigations.

Your AI Coding Assistant Has Potential Issues You Need to Be Aware of.

1.

It Has Issues With Predictability, Reliability, and Consistency.

Change one small word, e.g., type

Remove all items
instead of
Delete all items

...and you can get different results.

Repeat an error in your code, and you risk getting repeated errors in recommendations.



2.

There Are No Secure Defaults

The default code suggestions may be vulnerable. The suggested libraries may be insecure, out-of-date, deprecated, or unsupported.



3.

It Lacks Contextual Knowledge of Application Architecture (and can't see the forest for the trees)

The tools lack the contextual knowledge needed to provide more applicable suggestions. So, if you're working on a larger architecture, it won't get the bigger picture and adjust suggestions accordingly.



4.

You Depend on It When Navigating Unfamiliar Territory (but if it gets it wrong, you won't know)

It may help you navigate unfamiliar territory e.g., new programming language, but when it gets something wrong, the developer may not catch it due to their lack of familiarity with the language.



5.

...And You End Up Always Trusting the Default Suggestions from Your Automated Copilot

It's called automation bias and a way that potential vulnerabilities can enter the code base.



6.

Your AI Assistant Can Give Inaccurate Explanations

Just like a human, the tool can incorrectly analyze code or summarize changes incorrectly. Meaning your explanations or documentation will be inaccurate.



7.

It's Delivered as-a Service Which Could Lead to Data Leakage and Privacy Issues

You have no control over how your data is collected, stored, or used. AI coding assistants are hosted on third-party sites - Microsoft/GitHub, OpenAI, etc. They decide what data they use or share, which can lead to issues with loss of sensitive data and intellectual property.



Strategy For Mitigating Risks

Although automated coding assistants are relatively new, many existing tools and processes can address these new risks.



Read the report to find out more