Maze Launches Maze Code, Extending Its AI Security Agents from Cloud to Code

Maze is expanding its platform to two new products, extending the agents that secure its customers' cloud to the code they write and the dependencies they use.

Maze agents reason over your code, cloud, and business context to prove which findings are exploitable in your environment.

LONDON, UNITED KINGDOM, June 23, 2026 /EINPresswire.com/ -- Maze, the company building AI agents to secure cloud and code, today launched Maze Code, a suite of products that use AI agents to investigate every vulnerability in a team's dependencies (AI-SCA) and the code they write (AI-SAST), separate noise from risk, and automate remediation. Together with Maze Cloud, this launch makes Maze the first security platform to investigate every vulnerability with AI agents across both code and cloud on a single engine. Maze helps teams find and fix the vulnerabilities that matter.

Maze agents understand your code and environment like your best developer or security engineer. They understand the team's code, cloud, compensating controls, and business context, then prove which findings are exploitable in their specific environment. When one is, the agents trace its root cause, find and verify the fix, then deliver it as a pull request, use inside a coding agent like Claude, Cursor, or Windsurf, or a ticket routed to the developer who owns the code.

> Code security must move from rules to AI, but it's unpredictable. Maze Code shares our cloud product's foundation, proven on millions of investigations, so teams get AI code security they can rely on."
>
> *Harry Wetherald, Co-founder/CEO*

More code, faster attackers

Application security is being squeezed from two directions.

Frontier AI models give attackers the power to find and exploit flaws at unprecedented speed, while coding agents let teams ship more code, faster, with less review. Risk rises on the outside as the attack surface grows on the inside. The old approach to code security doesn't work anymore.

Legacy SCA and SAST scanners match findings against static rules, flooding engineers with noise without telling them what actually matters. 80 to 90 percent of vulnerabilities aren't exploitable, so teams spend most of their time on findings that were never a real threat.

It’s clear that code security needs to move from rules to AI. But AI is unpredictable and expensive, and a lot of teams are still struggling to make the move. We built Maze Code on the same foundations as our cloud product, so teams get code security results they can trust.

More than "AI-powered"

Every security product claims to use AI now, but agents are unpredictable, expensive, and hard to build well. This is why so many AI tools demo well and fall apart in production. Rather than bolt agents onto a legacy scanner, Maze built a platform designed around agents trained on specific security tasks. Over two years building Maze Cloud, the company trained its agents on millions of real investigations, evaluated against verified outcomes daily. Maze Code builds on that same foundation, in three ways:

Deeper, more accurate investigations. You can trust every verdict. Most tools stop at reachability. Maze agents treat it as the first signal, then weigh your configuration and surrounding controls to prove what's exploitable. Multiple layers of validation catch errors before they compound, bringing hallucinations down to nearly zero.

Expert agents, affordable at scale. Nothing goes uninvestigated. Maze trains its agents to investigate like expert security engineers, then to do it efficiently. They learn when an expensive model is worth it and when a cheaper one will do. Now you can investigate every finding, not just criticals, at scale.

Unified code and cloud context. One picture of risk. When run together, Maze Code and Maze Cloud draw on one model of the environment, so a finding in one informs the other. If a vulnerable function sits in code, Maze agents use cloud context to judge the real risk it carries, not just its severity on paper. You get one unified ticket with the fix, instead of the same issue alerting twice.

How it works

Maze Code ingests findings from the scanners you already run, or acts as the scanner itself.

Maze agents investigate each finding before alerting your team. They apply human-like reasoning to every vulnerability, gathering context from your code and cloud.

For known dependency vulnerabilities, Maze agents build AI call graphs to trace reachability through the dynamic calls rules-based scanners give up on. If a vulnerability is reachable, they go one step further and weigh the finding against build and runtime context to prove what's exploitable, separating real risk from noise.

In your own code, the hard part is understanding how the code actually works. Rules-based scanners can't do that, which is why no one solved this before AI. Maze agents read your code's structure and data flow to understand what it does. They catch standard issues like SQL injection, XSS, and hardcoded credentials, and go further to surface the novel vulnerabilities and business logic flaws that pattern-matching scanners miss.

"This SAST finding is exactly the kind of finding that we were hoping to get from a pentest. So very much kudos to you. This is awesome," said Nathan Cooke, Engineering Manager, Product Security, Alloy.

When a vulnerability is exploitable, Maze agents trace its root cause, and deliver a verified fix to the coding agent or developer responsible for the code. When several findings share a root cause, they prioritize remediation with a single fix. When a vulnerability isn't exploitable, they close it before it reaches your team. Every verdict comes with the evidence behind it.

Early results suggest that ~90% of CVEs are not exploitable in context. Maze Code has already found CVEs in open-source projects and surfaced vulnerabilities in customer environments including MFA bypass and cross-tenant data access, all delivered with a verified fix.

Maze Code works on its own or alongside Maze Cloud. To see it, book a demo at mazehq.com/contact.

About Maze

Maze is the first security platform to deeply investigate vulnerabilities with AI agents across both code and cloud on a single engine. Maze agents understand your environment and prove which findings are exploitable. If a finding is exploitable, they trace its root cause and find a fix. Then they ship that verified fix directly to the developer or coding agent responsible.

Learn more at mazehq.com.

Joseph Barringhaus
Maze
email us here

Visit us on social media:
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/921362597

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.