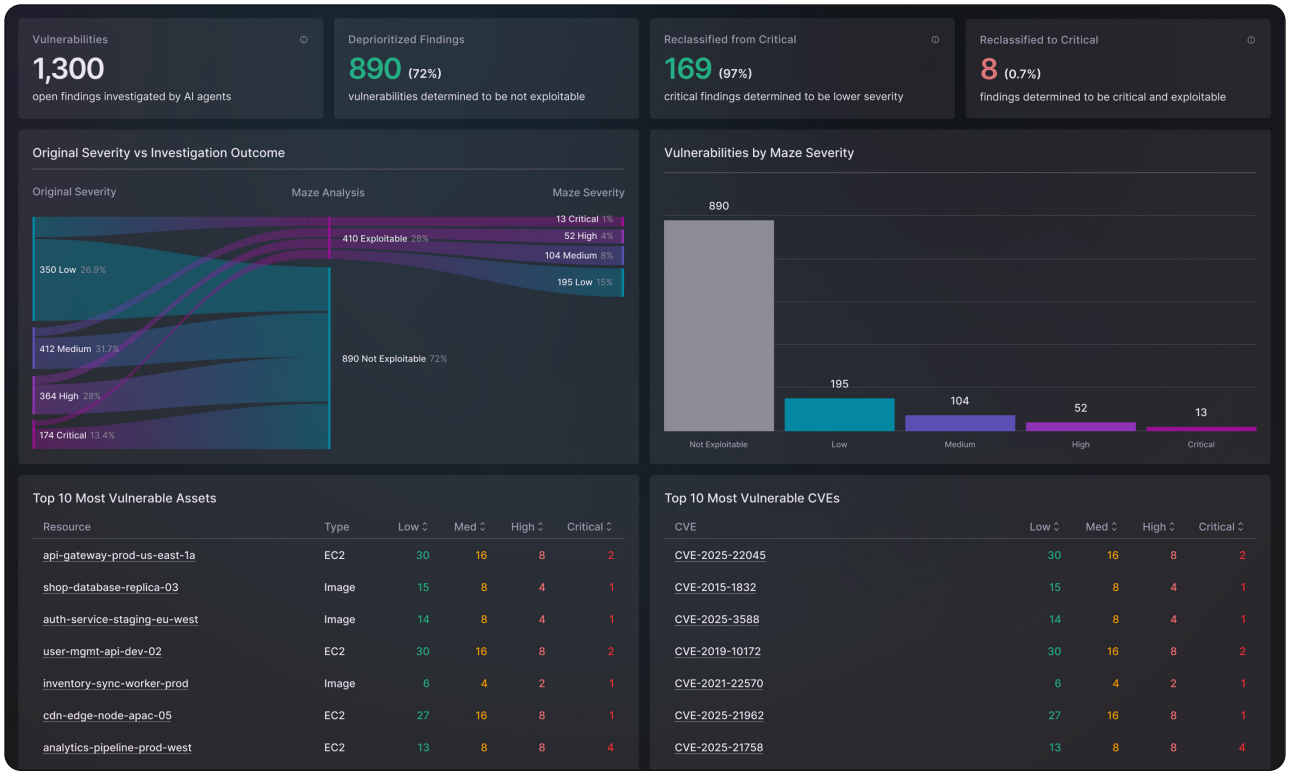
maze

Latio
CLOUD SECURITY SEGMENT LEADER
2025

Maze has built an agentic approach to vulnerability management by giving AI agents resources to investigate CVEs and your environmental context to determine the true priority of a vulnerability. A struggle in vulnerability management is the unique nature of every CVE - no single method of reachability can ultimately account for every edge case in the way AI can.

Maze adapts to the specifics of your environment, investigating CVEs on a case by case basis, the way a highly skilled product security engineer or developer would. Whether investigating containers or other cloud workloads, Maze dives into your environment in a way that traditional tooling categorically cannot, capturing the nuance and context needed to understand real exploitability and severity.



By giving AI the freedom to investigate every vulnerability, teams are unconstrained by the limits of traditional approaches to vulnerability research. Each CVE receives a thorough analysis of how it would be exploited, alongside evidence to attest if the vulnerability is a true or false positive. Maze is focused on the main pain points vulnerability management teams face every day: understanding what findings mean, separating the true positives from all the noise, analyzing the remaining exploitable issues to prioritize what matters, and attesting to the false positives for auditors.

The Benefits of Maze

Save Developers & Security Time

by enabling them to only focus on issues that matter, with steps to reproduce the attack, full vulnerability analysis, and prioritization based on risk to your environment.

Reduce Vulnerability Workloads

with best-in-class false positive detection, rule out massive numbers of false positives.

Understand Every Weakness

with thorough exploitability analysis and control assessments, you can accurately prioritize every potential threat vector.