WIZ + maze

Executive summary of the integration

Maze ingests Wiz vulnerability findings and investigates whether each one is actually exploitable in your environment. Maze AI agents start with Wiz's deep cloud visibility, then layer on additional runtime and static analysis from your cloud environment without deploying any sensors. Each vulnerability is classified as exploitable or not exploitable, with a full audit trail behind every decision. For exploitable findings, Maze assesses business impact and likelihood to prioritize based on real risk, then gives engineering the context and steps to remediate faster. Security teams focus remediation on what matters most and generate compliance-ready proof for anything deprioritized.

Market challenge

CVE volume grows over 40% yearly, while security teams don’t grow at the same rate. Most vulnerabilities can’t be exploited given an organization's specific configuration. Maybe the vulnerable library isn’t loaded, or a module is disabled. But proving that requires an investigation that teams just don’t have time for. Maze AI agents with great context from Wiz and your cloud can do that investigation at scale.

Key benefits of the integration

- **Use AI Agents to investigate every Wiz finding** with runtime and static context from your cloud environment to determine whether exploitation is technically possible
- **Triage and prioritize at scale with context,** classifying findings as exploitable or not exploitable in your environment, and prioritizing by real business impact and likelihood
- **Accelerate remediation with Maze** agents that think like developers, use cloud environment context, deliver fixes tailored to your stack, and route issues to the right owner
- **Generate compliance-ready proof** with a full audit trail in Maze showing the evidence and reasoning behind every agent’s decision, from deprioritized findings to escalated risk

The “Better Together” Story

Wiz set the standard for agentless cloud security, combining deep visibility with coverage across VMs, containers, and serverless workloads. That visibility, combined with Wiz's risk prioritization, gives teams a strong foundation. Maze adds deep investigation with AI agents to prove exactly what can and can't be exploited in your environment.

Maze ingests every Wiz finding and investigates whether exploitation is technically possible based on your configuration. Maze gathers its own runtime and static context from your cloud, without any sensors, reasoning like an expert security engineer. Each finding is classified as exploitable or not exploitable with full transparency. When exploitable, Maze assesses impact and likelihood to prioritize based on real risk, then gives engineering the context to remediate faster.

Wiz finds and prioritizes vulnerabilities with unmatched visibility. Maze investigates each one to prove what's exploitable and helps you fix it faster. Together, security teams get the full picture from detection to remediation.

Use Case Overview, challenge and solution

Use Case: Vulnerability Prioritization, Investigation, and Remediation. Security and engineering teams need to determine which vulnerability findings need immediate action, which can be safely deprioritized, and how to fix what matters, without manually investigating each one.

Challenge: Prioritization helps teams focus, but proving a vulnerability isn't exploitable requires deep investigation. A 9.8 CVSS vulnerability might be technically impossible to exploit because a required library isn't loaded or a module is disabled, while a 5.0 finding might be a serious risk given how the asset is deployed. Without deep investigation, teams either waste resources patching everything or risk missing the real threats in the noise. And when they do identify what to fix, teams need clear guidance, not a research project.

Solution: Wiz continuously scans cloud workloads and identifies vulnerabilities with deep cloud context. Maze then ingests those findings and investigates each to determine whether exploitation is technically possible in your environment. Each asset is independently investigated, gathering runtime data directly from your cloud without deploying any sensors. Each investigation determines whether a vulnerability is exploitable or not, with a full audit trail to review the decision. Maze then evaluates blast radius and business impact to prioritize vulnerabilities, just like your best security engineer would. For exploitable findings, Maze delivers remediation guidance that fits your environment and routes it to the right owner. Security and Engineering start from a place of deep understanding, not a request to investigate.

Integration Architecture Diagram

About Wiz

Wiz is on a mission to transform cloud security for customers – which include 50% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.

About Maze

Maze builds AI agents to investigate, triage, and remediate cloud vulnerabilities. Vulnerability management is broken, and security teams deserve solutions that can think like them. AI is how security teams finally get ahead. Maze is how teams prove what's actually exploitable and find the true severity. Security can focus on real risk, while engineering gets the context and steps they need to fix issues faster.