WIZ + HCP Terraform

The Wiz and HCP Terraform integration bridges Infrastructure-as-Code (IaC) and cloud resources, providing comprehensive code-to-cloud visibility. This collaboration enables organizations to proactively prevent risky infrastructure changes before deployment and swiftly remediate risks by tracing them directly to their source in code, eliminating drift. By unifying prevention and remediation, the integration reduces security toil, offers developers precise feedback, and aligns cloud environments with their code definitions.

Benefits of the integration

- **Gain visibility:** Wiz's code-to-cloud mapping capabilities bring IaC context directly into the Wiz Security Graph, providing unparalleled root-cause visibility and AI-powered remediation.
- **Close the gap:** Connecting Wiz to HCP Terraform directly addresses the disconnect between IaC definitions and live cloud resources, providing a clear, end-to-end view of how every resource was deployed and who owns it.
- **Improve efficiency:** Developers gain precise, contextual feedback, enabling them to fix issues before applying Terraform plans with confidence and reducing time spent on investigating production problems later.
- **Achieve consistency & scale:** Wiz ensures consistent policy enforcement across code, pipelines, and runtime, helping security teams scale by working more closely with engineering.

Market challenge

Modern cloud environments, heavily reliant on IaC, offer speed and control but also introduce new layers of complexity and risk. Organizations commonly face a disconnect:

- **Siloed tools and scanners:** CSPM tools monitor runtime environments, while IaC scanners analyze code. These tools operate independently, leading to disjointed workflows and findings.
- **Lack of root cause analysis:** CSPMs detect issues in production (e.g., open S3 buckets, over-permissive IAM roles) but struggle to trace them back to their originating code.
- **Missing context:** IaC scanners identify risky patterns in code but often lack runtime context to determine if these issues actually reach production. Developers receiving alerts they don't trust.
- **Drift:** This disconnect results in fixes often being applied directly in the cloud console, introducing configuration "drift" and breaking GitOps workflows.

The better together story

Wiz and HCP Terraform unite to provide a comprehensive security solution that spans the entire development lifecycle, from the first line of code to live production environments. Wiz provides immediate, full-stack visibility into cloud workloads, identifying vulnerabilities, misconfigurations, and secrets exposures, and mapping potential attack paths. Terraform, instrumental in democratizing IaC, streamlines cloud infrastructure deployment through automation.

Use case overview, challenge, and solution

CHALLENGE

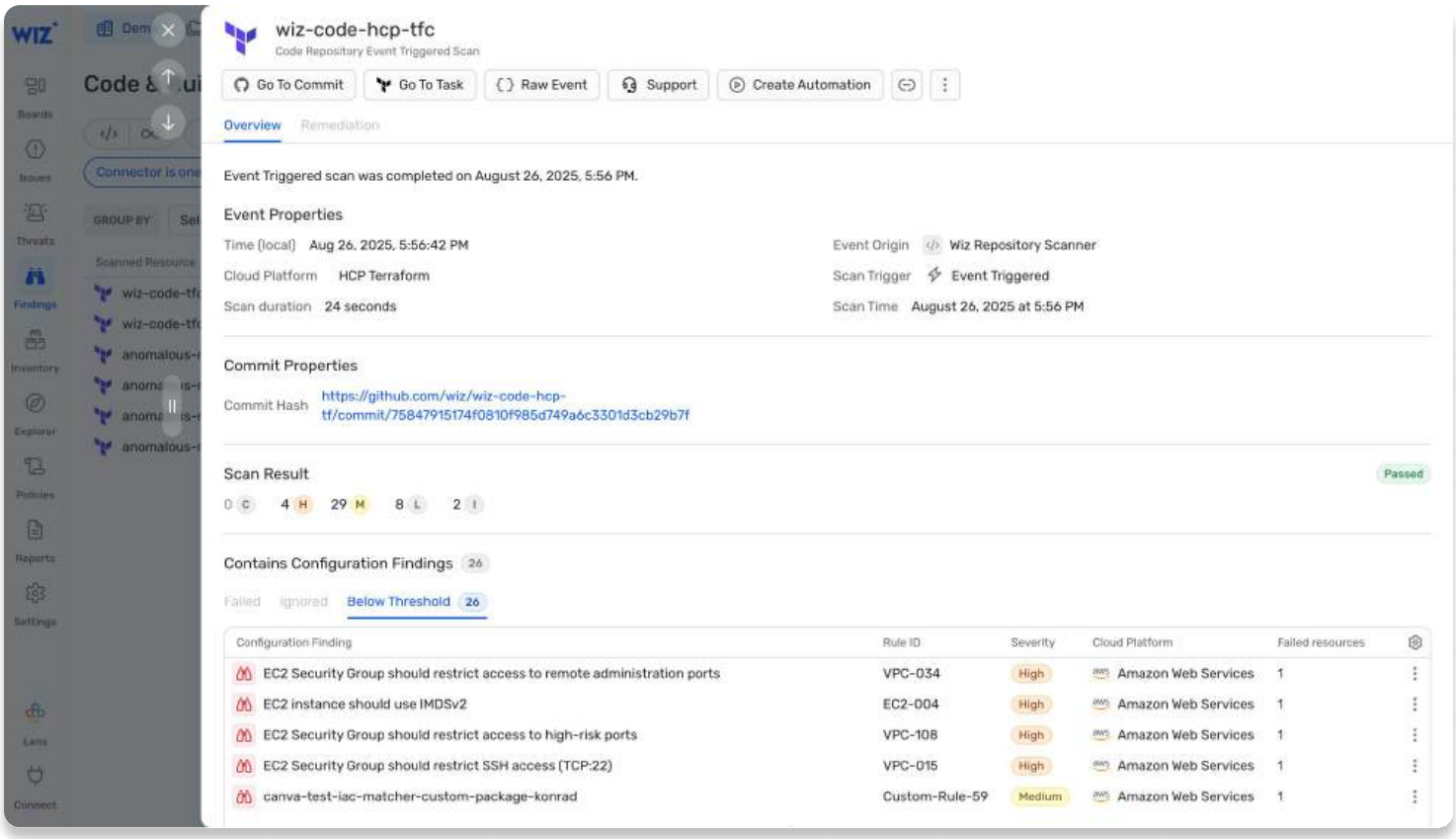
Catching infrastructure risks before they reach production

Security workflows are fragmented: CSPM tools detect misconfigurations in production, but too late. IaC scanners identify risky patterns but lack context on whether they ever make it to the cloud. This results in the inability to pinpoint root causes, low-context alerts, and fixes creating drift. The rapid pace of IaC, especially with AI copilots, allows more misconfigurations and secrets to slip through undetected.

SOLUTION

Wiz HCP Terraform integration for Terraform post-plan scanning

The integration embeds security directly into the Terraform workflow. Wiz acts as a run task within HCP Terraform Cloud and Terraform Enterprise, automatically scanning every Terraform plan before it gets applied. This critical check allows Wiz to apply a comprehensive IaC and secrets scanning rules, enforced by a unified policy engine. Configure a rule once (e.g., "S3 buckets must not be public"), and it will consistently flag a bad Terraform declaration in a pull request, block a risky plan during a run, or identify a misconfiguration already live. Violations surface directly within Terraform runs and Wiz with clear context and fix guidance, enabling developers and platform engineers to fix issues in their flow of work, pre-deployment.



CHALLENGE

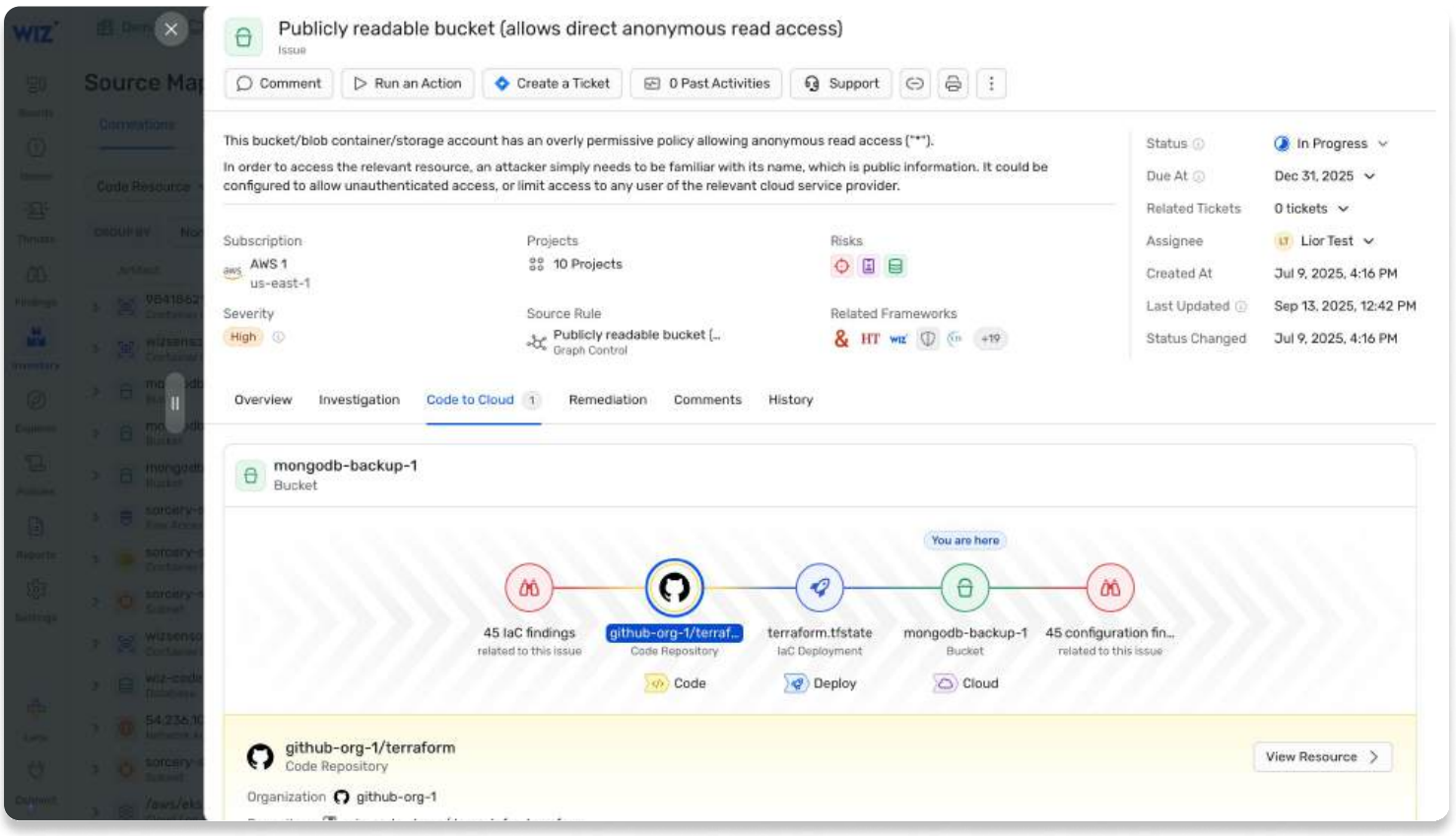
Tracing infrastructure risks back to IaC misconfigurations and their owners

When a misconfiguration is detected in a live cloud environment, like an overly permissive IAM role, security teams often face a challenge of figuring out how it got there and who is responsible for it. This leads to delayed remediation, and an inability to fix issues at their origin. Fixes end up being "hot-patched" directly in the cloud console, introducing drift and breaking the integrity of IaC as the single source of truth.

SOLUTION

Map code to cloud and back

Integrating Wiz and HCP Terraform helps map code to cloud and back. Wiz Code scans Terraform code in version control systems like GitHub, resolves variables and modules for accuracy, and uses the Terraform state backend to link live and deployed resources to the specific IaC files that created them. This full lineage appears on the Wiz platform on the resource's details and is explorable in the Wiz Security Graph. Code-to-cloud empowers developers to open a targeted pull request, and to make the fix at the source, avoiding drift.



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 CNAPP platform delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context, less noise, so that security teams can focus their time on what matters most.

About HashiCorp (An IBM Company)

HashiCorp, an IBM company, helps organizations automate hybrid cloud environments with Infrastructure and Security Lifecycle Management. HashiCorp offers The Infrastructure Cloud on the HashiCorp Cloud Platform (HCP) for managed cloud services, as well as self-hosted enterprise offerings and community source-available products.