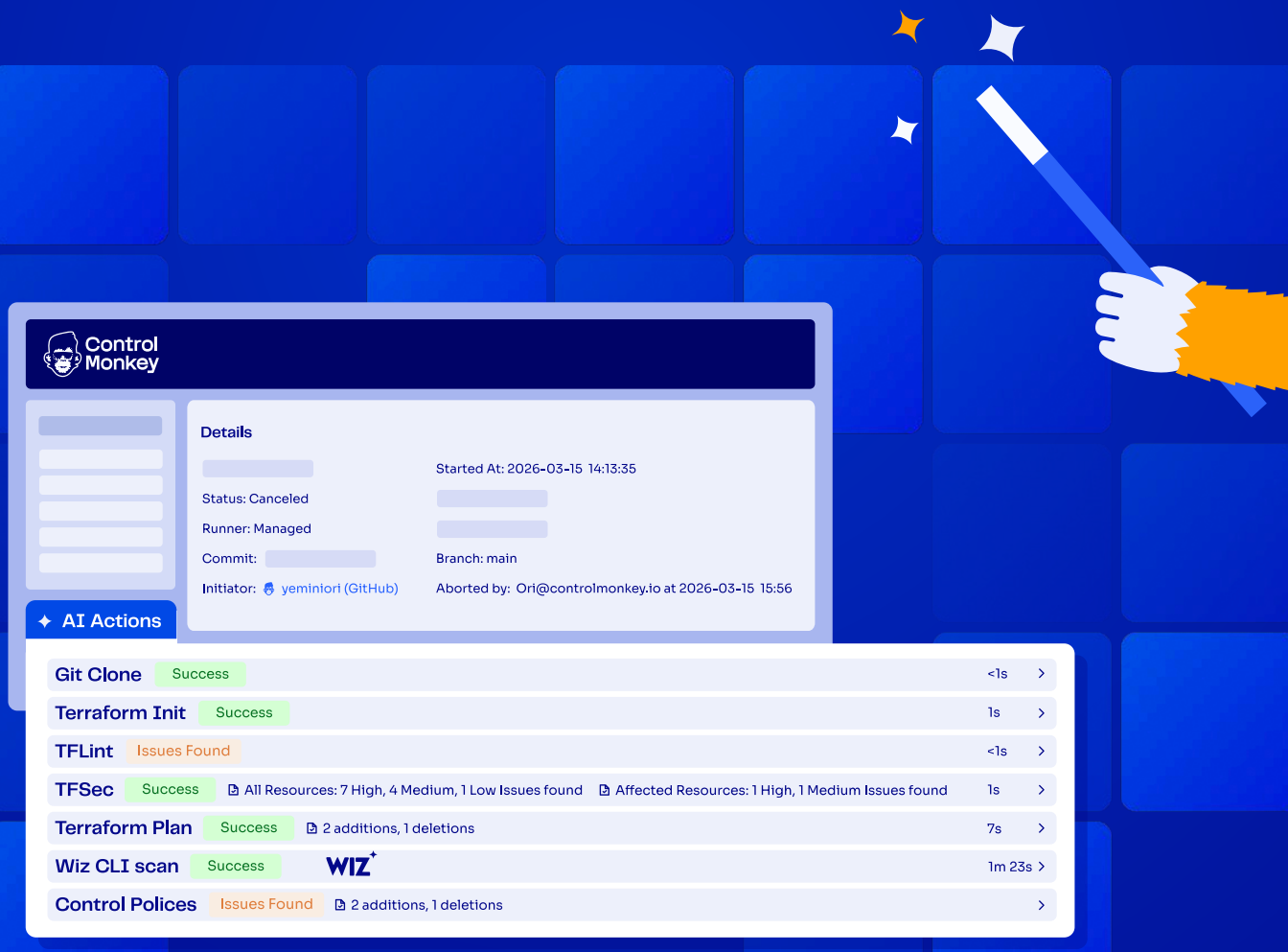
Wiz + ControlMonkey Integration

How Wiz and ControlMonkey validate risk, enforce guardrails, and prevent unsafe cloud changes before deployment

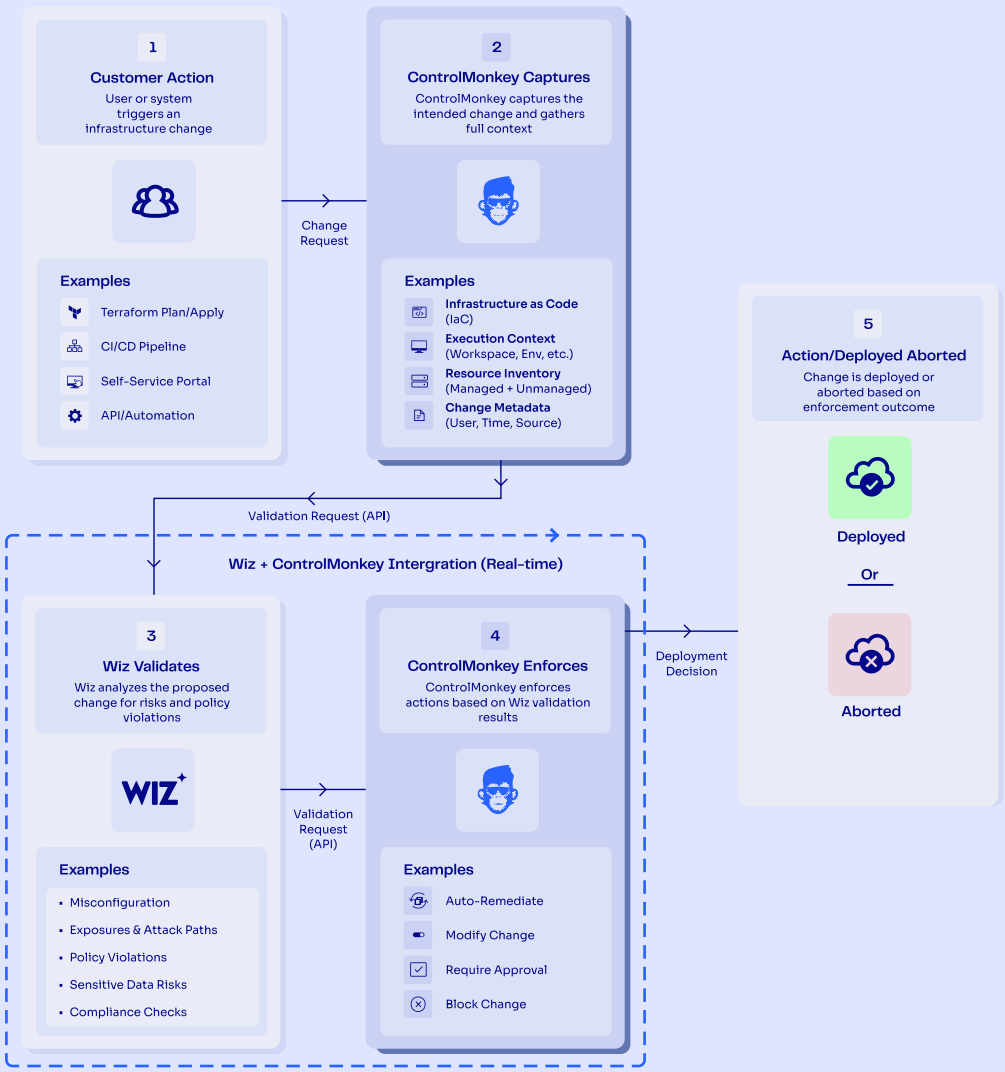


Wiz + ControlMonkey Integration Flow

Real-time risk validation and enforcement for every infrastructure change

Integrates with: Wiz Cloud Wiz Code

From Cloud Risk Detection to Governed IaC Remediation



Executive Summary of the Integration

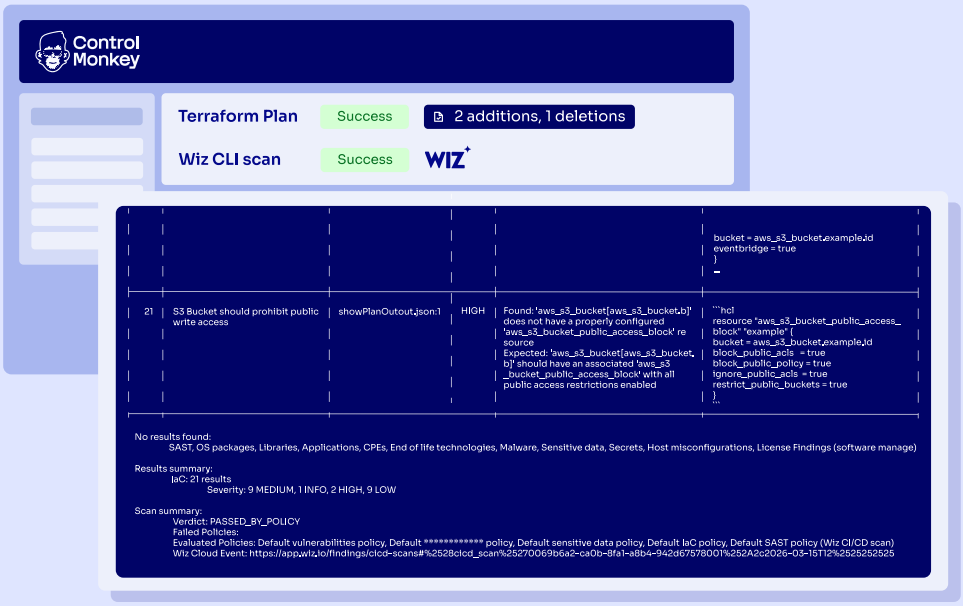
The Wiz and ControlMonkey integration bridges Infrastructure as Code (IaC) with real-time cloud risk visibility, connecting security insights to the full cloud environment - not just what's defined in code.

Wiz identifies misconfigurations, exposure paths, and risks across cloud and SaaS environments, while ControlMonkey provides a governed automation layer that continuously maps live infrastructure to IaC (Terraform, OpenTufo and Terragrunt), including unmanaged and drifted resources.

By translating risk findings into controlled, code-based remediation, teams can reduce manual effort, eliminate blind spots beyond IaC, and maintain secure, consistent cloud environments at scale.

Market Context

Organizations struggle with fragmented visibility across their cloud environments. Infrastructure as Code (IaC) tools and cloud security platforms operate in silos, making it difficult to trace risks back to their source or understand their real impact. This lack of context leads to delayed remediation, manual fixes, and increased exposure to security threats.



Key Benefits of the Integration

1. **Gain full visibility**
   a. Connect IaC with live cloud environments to see what's deployed across managed and unmanaged resources—and where risks exist

2. **Close the IaC-to-cloud gap**
   a. Continuously align infrastructure code with live cloud environments, including unmanaged and drifted resources

3. **Improve team efficiency**
   a. Provide actionable insights that accelerate investigation and remediation

4. **Drive consistency at scale**
   a. Standardize configurations and enforce policies across environments

5. **Automate drift remediation at scale**
   a. Detect and safely reconcile configuration drift by aligning cloud environments back to approved IaC

The “Better Together” Story

Wiz and ControlMonkey bring together cloud risk visibility and Infrastructure as Code (IaC) execution to close the gap between detection and action. Wiz provides deep visibility into cloud environments, identifying misconfigurations, exposed assets, and attack paths across both managed and unmanaged resources.

ControlMonkey extends these insights into a governed automation layer, continuously mapping live infrastructure to IaC and enabling teams to safely remediate risks through controlled, code-based workflows.

Together, organizations move beyond identifying issues to consistently resolving them —reducing manual effort, eliminating blind spots, and maintaining secure, compliant cloud environments as they scale.

Use Case Overview

Challenge

Security teams identify misconfigurations and risks across cloud environments, but struggle to remediate them efficiently. Many resources exist outside IaC or have drifted from code, making it difficult to trace issues back to their source and fix them safely. As a result, remediation is often manual, reactive, and inconsistent—introducing delays and increasing operational risk.

Solution

With the Wiz and ControlMonkey integration, security findings are directly connected to how infrastructure is defined and managed. Wiz continuously scans cloud and SaaS environments to detect risks, while ControlMonkey maps these findings to Infrastructure as Code—including unmanaged and drifted resources. Teams can then apply governed, policy-driven remediation, automatically aligning cloud environments back to approved configurations through controlled IaC workflows.

Impact

Organizations can move from fragmented, manual remediation to a consistent and scalable model. Risks are not only identified but resolved in a repeatable way, reducing exposure and operational overhead. Teams gain confidence that their cloud environments remain aligned with IaC, secure by design, and resilient as they evolve.

Start with Free

Cloud Risk Assessment

Understand your cloud and IaC risk

What will you learn?

- **Can we restore our cloud configuration if something breaks?**
- **Where are your recovery blind spots?**
- **How exposed are we to extended downtime, audit risk, or operational failure?**

What You Get

- Visibility into which cloud and SaaS configurations are DR-ready - **and which are not**
- Identification of high-risk gaps that could delay recovery
- Actionable recommendations to improve your BCP

What's Required

Read-only access to selected cloud and SaaS accounts	**No agents to install, No infrastructure changes**	**No change to production systems**

Request your Cloud DR Readiness Assessment

Know where your disaster recovery plan protects you - and where it leaves you exposed.