# Fugue

## Infrastructure as Code Security

Secure your infrastructure as code (IaC) in development and CI/CD — and use the same policies to secure your cloud runtime.

### IaC Security Powered by Open Policy Agent

Fugue leverages the open source Open Policy Agent (OPA) standard for IaC and cloud infrastructure policy as code.

- Build IaC checks into git workflows and CI/CD pipelines with Regula—an open-source tool powered by OPA
- Apply the same policies to your IaC and cloud environment with Fugue's Unified Policy Engine for consistency and time savings
- Develop custom rules—including multi-resource checks—using Rego, the simple and powerful open source language of OPA

### Centralized IaC Security Management

Govern your IaC security for cloud resources, Kubernetes, and containers in one place and ensure consistent policy enforcement across the development lifecycle.

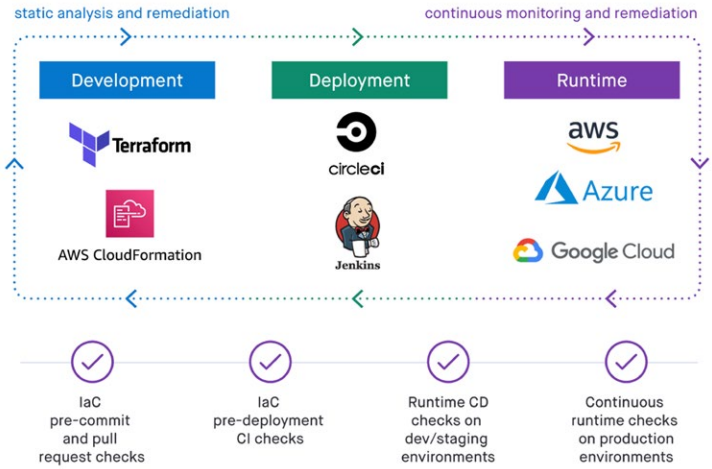
- Quickly onboard your code repositories to Fugue to establish full IaC security visibility
- View the results of security and compliance checks on IaC across your organization
- Access and export tenant-wide, IaC-specific security and compliance reports

### Developer-Friendly Tools and Integrations

Ship code faster and more confidently in the cloud with rapid developer feedback and CI/CD checks for IaC security.

- Check IaC templates before they're committed to a Git repository with open source command line tools
- Integrate IaC security to your Git workflows, whether you use GitHub, GitLab, or a private repo
- Automatically catch IaC policy violations in CI/CD pipelines

**Regula Policy Engine** for infrastructure as code and cloud security




Terraform · AWS CloudFormation · kubernetes · docker · aws · Azure · Google Cloud

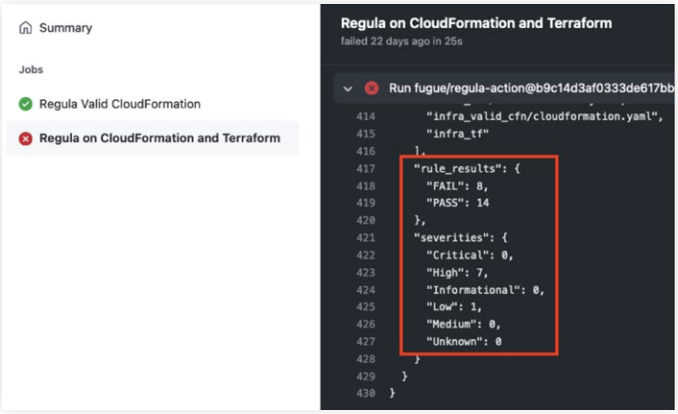
# Fugue

Infrastructure as Code Security

## Security for Cloud, Containers, and Kubernetes

Validate IaC for your infrastructure stack with pre-built compliance libraries and your custom enterprise security policies.

- Evaluate Terraform HCL, plan files and modules to avoid cascading misconfiguration vulnerabilities
- Validate AWS CloudFormation templates—whether YAML, JSON, composed by hand, or generated by the AWS CDK.
- Check Kubernetes manifests and Dockerfiles to ensure that clusters and container images are appropriately configured




## Comprehensive Compliance Coverage

Leverage hundreds of out-of-the-box policies mapped to common compliance standards.

- Take advantage of hundreds of best-in-class cloud infrastructure rules maintained by Fugue's team of cloud security experts.
- Detect dangerous IaC vulnerabilities that span multiple resources, not just single-resource issues.
- Secure IaC according to industry compliance standards—and Fugue Best Practices to catch vulnerabilities that compliance can miss.

SOC 2 | NIST 800-53 | GDPR | PCI | HIPAA | ISO 27001 | CSA CCM
CIS Controls | CIS Docker | CIS Benchmarks for AWS, Microsoft Azure, Google Cloud, Docker, and Kubernetes

## Visualize Your IaC and Security

Understand your cloud infrastructure and security posture pre-deployment with interactive IaC diagrams.

- Generate interactive maps of your IaC templates and security posture
- Zoom in to inspect configuration details, resource relationships, and policy violations
- Export your IaC diagrams and include them in infrastructure planning and approval processes

**Getting Started with Fugue for IaC and Cloud Security** It takes just 15 minutes to get up and running with Fugue. Get started for free at **www.fugue.co.**

The Fugue SaaS platform secures the entire cloud development lifecycle—from infrastructure as code through the cloud runtime. Fugue empowers cloud engineering and security teams to prove continuous compliance, build security into cloud development, and eliminate cloud misconfiguration. Fugue supports Amazon Web Services, Microsoft Azure, and Google Cloud, and provides one-click reporting for CIS Foundations Benchmarks, CIS Controls, CIS Docker, CSA CCM, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2.

Inquiries: hello@fugue.co
Call us: 1.844.463.8483