SOLUTION BRIEF

# Lacework infrastructure as code (IaC) security

Develop and run secure cloud infrastructure

## OVERVIEW

### The need for simple, automated security within development

Infrastructure as code (IaC) has changed the game when it comes to provisioning cloud infrastructure. IaC automates the configuration and provisioning of infrastructure through written, human-readable code, enabling faster delivery of cloud-native applications.

While IaC speeds the deployment of cloud infrastructure, if left unchecked, it can introduce dangerous security and compliance risks within production cloud environments. A recent ESG survey found that 83% of organizations using IaC are experiencing an increase in cloud misconfigurations causing security incidents.[1]

Organizational silos and a growing skills shortage compound this problem. Security teams grapple with a lack of visibility and control over code development, including IaC. Meanwhile, developers and platform engineers often lack security expertise, have difficulty navigating fragmented IaC security tools, and work in increasingly decentralized roles across the organization.

## THE LACEWORK SOLUTION

### Respecting the developer experience

The Lacework Polygraph® Data Platform extends automated security and compliance checks of IaC early in the development process to prevent misconfigured cloud services from being deployed. Lacework integrates IaC security seamlessly into developers' existing toolchains, so they don't have to switch out of their workflows to secure their code.

Within minutes, Lacework can be connected to code repositories like GitHub, Gitlab, and Atlassian Bitbucket, or into CI/CD pipelines such as GitHub Actions, CircleCI, TravisCI, and Jenkins, using the Lacework CLI. We support templates such as Terraform, AWS CloudFormation, and Kubernetes/Helm, in addition to the ability to scan Dockerfiles. Teams can use Lacework to automatically discover IaC templates and code repos used across the organization.

## Challenges

- Cloud configuration has been automated with IaC, but security has not
- Insecure IaC code can propagate to hundreds or thousands of instances
- Developers are not experts in IaC or security configurations
- Security lacks visibility and control over IaC security

## Benefits

- Dramatically reduce cloud risk by preventing non-compliant IaC from being deployed, and significantly lower the cost of fixing security flaws in production
- Empower developers to self-service the security of their code and increase their productivity with automated guardrails and actionable guidance that is tightly woven within their existing toolchains
- Give security teams centralized visibility and control of IaC security posture
- Ensure each developer automatically applies the latest security and compliance controls
- Eliminate chaos resulting from automating shift-left security at scale by maintaining a central policy repository

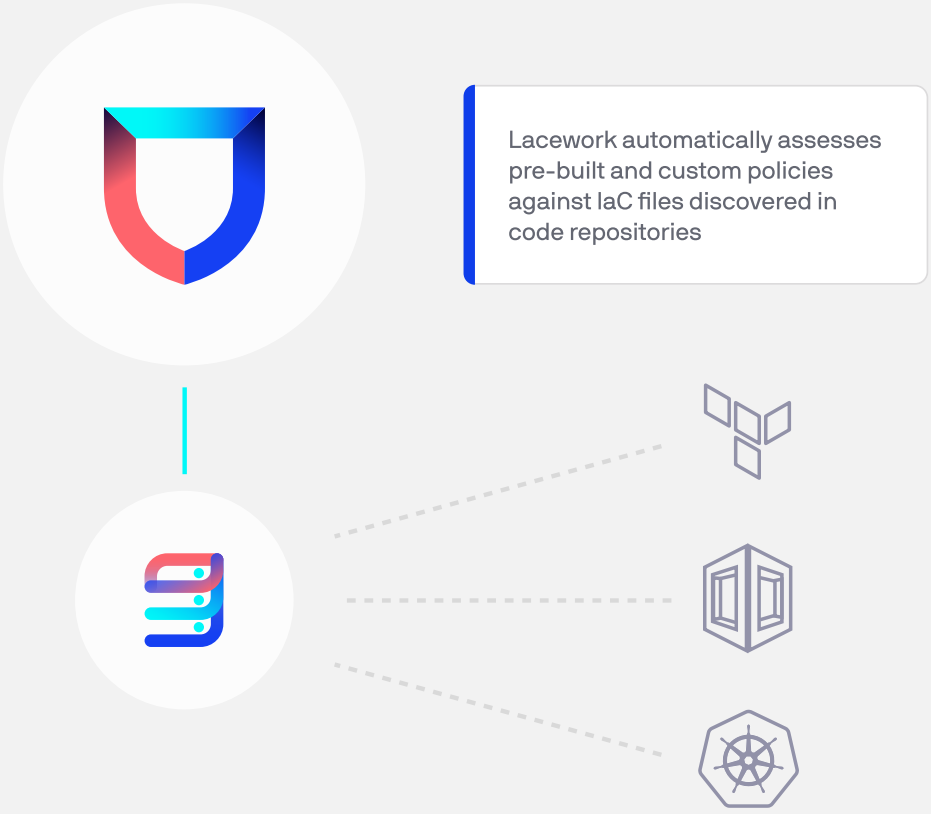
[1] *ESG Survey: Walking the Line: GitOps and Shift Left Security, 2022*

Lacework adds security guardrails that automatically and continuously scan IaC for policy violations and immediately alert developers as they are writing code. When IaC is submitted (pull request or commit) to a code repository, Lacework will automatically test it against any assigned security and compliance policies. Organizations can also use Lacework to test IaC once it has been packaged for delivery, to ensure production parameters, like us-west-1, are within policy.

Lacework provides hundreds of pre-built policies out-of-the-box, or teams can create their own custom IaC security policies to meet the specific requirements of their business.

All identified misconfigurations are recorded within the code repository, as well as the Lacework UI, to ensure both development and security teams have shared visibility into the security of the code. Developers receive immediate and automated remediation guidance for fixing the code, as well as the ability to auto-remediate with just one click. And for greater flexibility, Lacework enables teams to "block the build" on an alert, or to simply notify on and record the violation.

The ability to self-service security violations enables developers to work at their own pace, without having to wait the days or weeks it can typically take when security teams have to get involved.




## Key IaC security capabilities include:

- Continuous compliance monitoring with assessment of IaC code before it is deployed
- Automated remediation guidance for developers with one-click remediation option
- Build custom policies with OPA policy framework
- Easy integration into developer code repositories with option to automate security checks into CI/CD pipelines
- A single platform that delivers security from code to cloud, with a unified experience and data mode

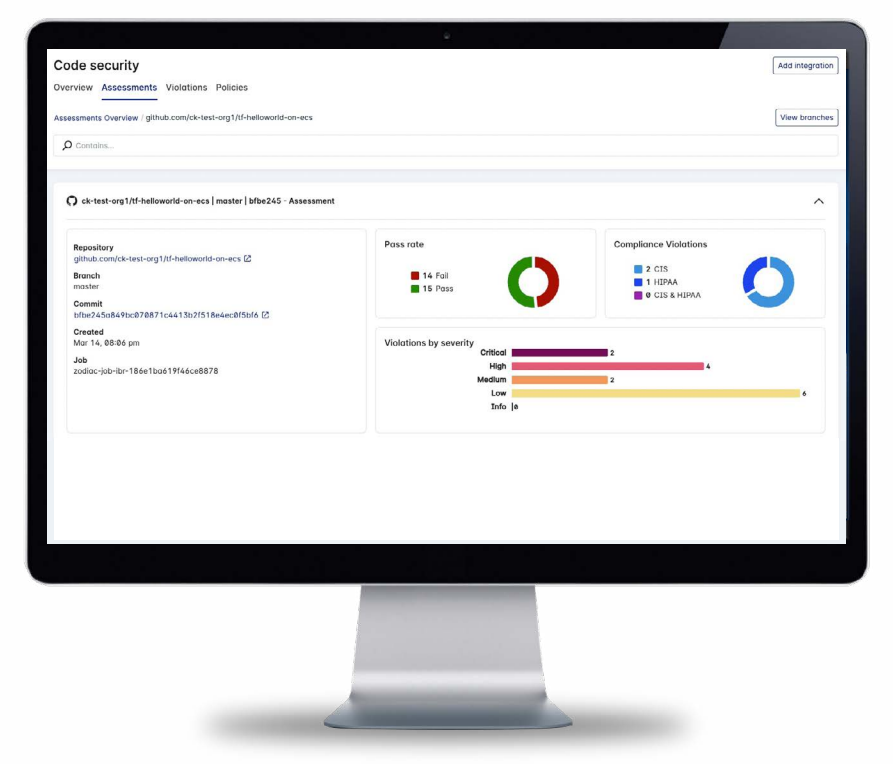



Figure 1: Assess IaC for misconfigurations and compliance violations in development

## Build and manage custom OPA policies

Embraced by a growing ecosystem of contributors, users, and technology providers, Open Policy Agent (OPA) is an open-source project that uses a single policy language and policy engine to manage security policy as code, across the cloud-native stack. Lacework offers an OPA framework that teams can use to build and manage custom policies. This framework exists to meet the unique needs of your organization and address any use case that falls outside the scope of pre-built policies, derived from industry standard best practices.

Our OPA framework enables policy to be managed as a first-class citizen, like application code, through developer workflows in Git. To write custom policies, the policy is first authored in Rego, and using the CLI, committed into Git, and then uploaded into the Lacework platform, and visible in its GUI. Once Lacework is connected to a repository, or an on-demand assessment is initiated, it will automatically validate every policy against each commit, and pull request. Lacework returns the assessment results for each action back to the Git repository so developers receive findings within their existing Git tools and workflows. If violations are identified, teams have the option of either blocking the request, or allowing it to pass with notification of the found violations.

Using the Lacework CLI, the policies are also uploaded into the Lacework platform. Lacework then verifies these policies against any new IaC actions within the attached repositories and build pipelines.

Custom policies can be useful for enforcing the proper tagging of IaC. For example, the security team could mandate tags for a financial application that uses sensitive information. Teams can write custom policies to ensure resources are properly tagged, and block code improperly tagged. Using the Lacework OPA framework, teams can easily manage and govern policy as cloud deployments scale and create a foundation for a unified policy architecture that spans every layer of the cloud stack.

> **"Lacework is one of the best security partners that we work with. The Polygraph Data Platform brings everything into one place, it's not piecemeal. The Platform not only consolidates tools but saves us a lot of time and money."**
>
> RUSSELL K, INFORMATION SECURITY ENGINEER, RAPIDSOS

“

As soon as Lacework added its IaC security feature, I jumped in and started using it. That’s been great, because rather than having to build infrastructure as code and finding an issue once we’ve deployed it, we get a pull request right away for critical issues. Previously, if an issue came up during deployment, that added another week of time just to remediate it, whereas now, Lacework lets us fix these issues in about an hour so we can keep working faster.”

NICK PARFAIT, HEAD OF ENGINEERING, AVENUE BANK

## Bridge the gap between security and development teams

The benefits of Lacework IaC security are not limited to developers. Security teams gain centralized visibility into IaC security violations, policies, exceptions, and more, to quickly investigate and report on cloud risk. For example, security teams can gain comprehensive visibility into hidden or unknown IaC files and code repos used across the organization. This is possible because Lacework aggregates all the data in a single platform that is accessible to all teams.

Organizations can improve operational efficiencies, remove traditional siloes, and quickly establish a DevSecOps framework. The platform allows security, compliance, development, operations, and other teams to collaborate more closely and understand what IaC policies are applied, what violations may exist, and the status of remediation efforts, no matter where they sit in the organization.

With Lacework IaC security, teams can build cloud environments securely without friction and achieve fast time-to-market delivery of applications and services. Lacework helps reduce exposure from cloud misconfigurations and significantly lowers the risk of security incidents in production, while saving substantial time and money on fixing security flaws.

Unlike fragmented IaC scanning point solutions, Lacework IaC security is built-in as part of our leading cloud-native application protection platform (CNAPP). This ensures that IaC security is consistently applied across application teams, always visible to security teams, and holistically managed in the context of an overall cloud security program.

## Want to learn more about Lacework IaC security?

To learn more visit our website, or contact us to schedule a demo or speak with our sales team.