

# Infrastructure as Code

## Secure your cloud environment

With the shift of applications to cloud environments and organizations heavily relying on cloud service providers, provisioning infrastructure has shifted from the IT team to developer and DevOps teams. Infrastructure as code (IaC) introduces a code-first approach that supports building and terminating cloud infrastructure components via cloud specification templates. IaC enables teams to efficiently automate environment provisioning at the speed required to get business done.

While IaC boosts efficiency, it can also amplify mistakes. By moving so quickly, a minor mistake by a DevOps admin at the template level can be propagated across the entire cloud infrastructure.

## Infrastructure as Code Security

Organizations need to bridge the gap between security, DevOps, and developer teams by providing the tools and guidelines to automatically scan their code for misconfigurations. They also need to provide mitigation guidelines that remediate discovered issues without disrupting workflows.

At the same time, security teams must prevent any vulnerabilities from reaching production branches.

Mend Infrastructure as Code helps organizations secure IaC templates and checks for security issues, compliance violations, and other misconfigurations. Developers can detect, track, and fix the misconfigurations as part of their normal workflow without leaving their code repositories to view results or set up a separate workflow to scan. This gives SecOps admins confidence in the security of infrastructure built and operated by DevOps.

## Key Capabilities

### Protect Your Production Environment

- Prevent insecure default configurations that could expose the entire organization with broad coverage of common IaC templates.
- Automate IaC security to prevent human error and reduce cloud-based threats.
- Detect issues before they reach production environments.

## Key Benefits

Detect IaC template misconfigurations before they are deployed and alert on any IaC policy violations

Secure your cloud, containers, and Kubernetes by scanning IaC for your infrastructure stack with pre-built compliance libraries

Identify security and compliance gaps earlier in the cloud development lifecycle (CLDC) to reduce your organization's risk

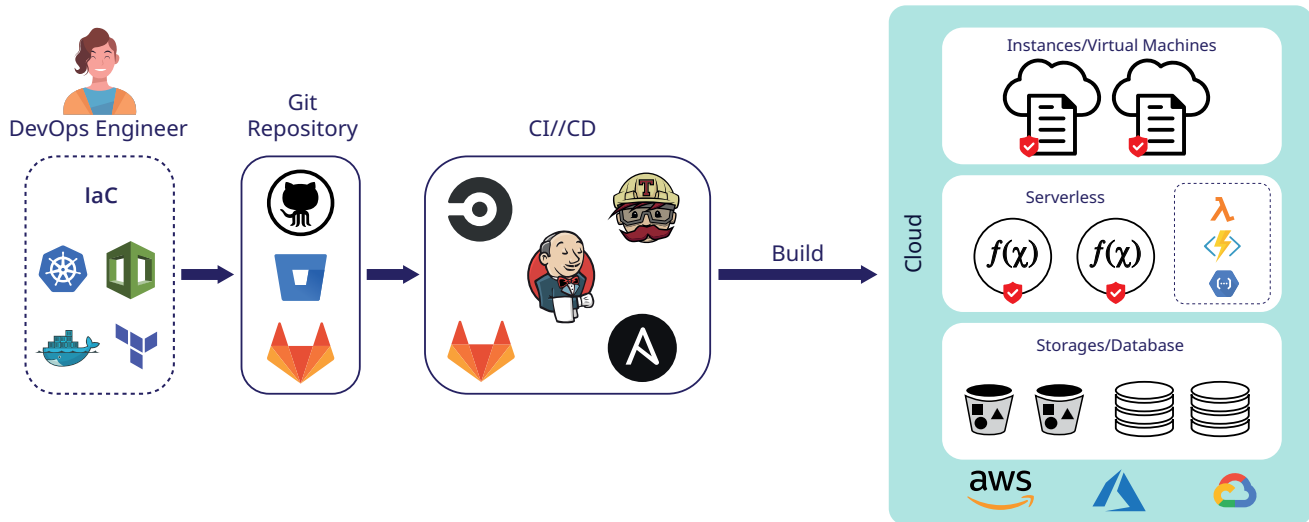
Gain confidence with the security level of your IaC templates and free your security teams to focus on runtime issues

## Provide Security for the Cloud, Containers, and Kubernetes

- Ensure your Kubernetes manifests and dockerfiles are configured according to SecOps guidelines to harden your clusters and container images.
- Secure Terraform, AWS CloudFormation IaC, and more in development.

## Infrastructure as Code Pipeline

Add security as code (SaC) guardrails to your cloud development lifecycle (CLDC) from code to the cloud.



## About Mend

Mend helps organizations accelerate the development of secure software at scale. We provide automated tools that bridge the security knowledge gap, integrating easily into the software development life cycle and going beyond detection with a remediation-first approach. Mend is built on the most comprehensive vulnerability database in the industry, providing the widest coverage for threats and attack vectors. Our solution helps enterprises reduce risk and increase the productivity of their security and development teams. For more information, visit [www.Mend.io](http://www.Mend.io)

## Related Resources

Learn more at [www.mend.io](http://www.mend.io)