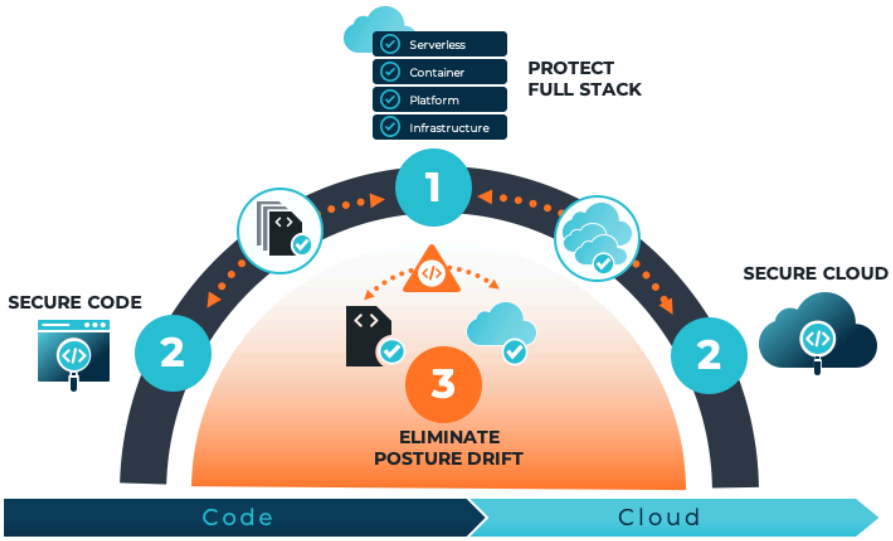
accurics™

Code to Cloud Security™

Immutable Security for Immutable Infrastructure

As organizations rapidly adopt new technologies such as serverless, containers, and servicemesh, cloud infrastructure is becoming increasingly "immutable": infrastructure is never modified after it is deployed. If something needs to be modified in any way, new infrastructure has to be provisioned through code. Traditional cloud security approaches are untenable for securing transient cloud native infrastructure. The only way to secure immutable infrastructure is to adopt a paradigm of immutable security which is based on three core principles:

1. Protect the full cloud native infrastructure stack including serverless, containers, platform, and infrastructure
2. Throughout the DevOps lifecycle from code (before infrastructure is provisioned) to cloud (after infrastructure is provisioned)
3. Eliminate risk posture drift over time by reconciling changes to cloud (provisioned infrastructure) that introduce risks with the baseline defined through code



"While infrastructure as code enables agility and reliability, it also provides an opportunity to embed security earlier in the DevOps lifecycle. Accurics reduces the attack surface by detecting risks in code before infrastructure is provisioned and flags changes to production that may introduce security posture drift."

— Talha Tariq,
VP & CSO @ HashiCorp

Embrace Cloud Native Technologies with Confidence

Accurics enables immutable security for immutable infrastructure so that organizations can embrace the latest cloud native technologies with confidence.

Cloud Integrity Assurance

Get real-time visibility into your topology defined through code to spot design issues from the get-go, monitor for design drift once your cloud infrastructure is deployed, and true up your code or cloud to prevent drift.

Compliance & Governance

Detect and resolve violations of common compliance and security best practices in code by leveraging 1500+ policies across 10+ standards such as SOC 2, GDPR, PCI, HIPAA, ISO, & CIS Benchmarks. This ensures that cloud infrastructure is compliant from the moment it is provisioned. Once deployed, the infrastructure is monitored against the same set of policies to detect and remediate any changes that introduce violations, making it easy to demonstrate compliance.

Breach Path Prediction

Accurics develops threat models by analyzing vulnerability feeds, IAM privileges, trust boundaries, and other data. Detect and remediate potential breach paths in the code before infrastructure is provisioned to significantly reduce the attack surface. Detect any subsequent changes to your deployed infrastructure that introduce risk and remediate via your existing workflow tools.

Accurics Integrates Into Your DevOps Lifecycle

Accurics connects to your code repository and scans code such as Terraform, Kubernetes YAML, Dockerfile, and OpenFaaS YAML. You can detect and remediate misconfigurations, policy violations, and potential breach paths before your cloud infrastructure is provisioned. It subsequently monitors your infrastructure deployed in AWS, Azure, and Google Cloud Platform to detect changes that introduce risk and create posture drift in the cloud from a baseline defined through code. You can remediate drifts by truing up your infrastructure code to reflect legitimate changes or redeploying your cloud from code to mitigate risks.