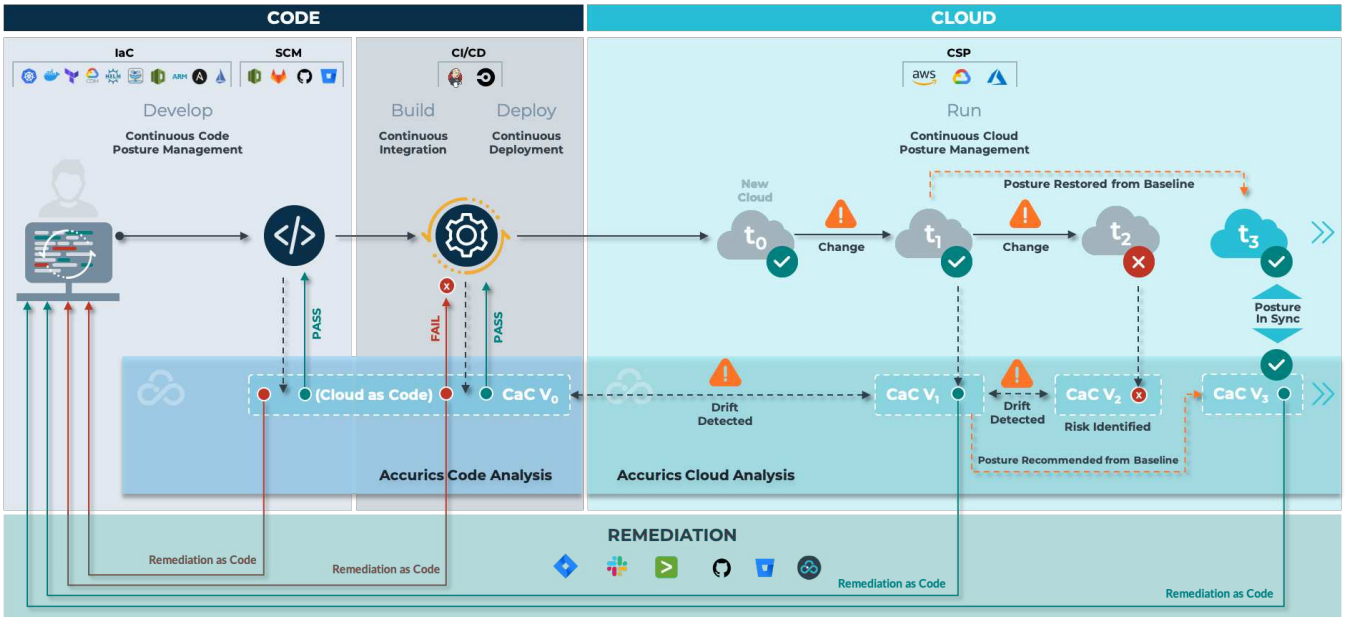
accurics™

Product Brief

# Securing Cloud Native Infrastructure

The adoption of cloud native infrastructure such as serverless, containers, and service mesh are enabling organizations to deliver new innovations to market. Unfortunately, over 30 billion records have been exposed in cloud breaches over the last two years and the velocity of these breaches continues to accelerate. Traditional cloud security approaches are becoming untenable for securing transient cloud native infrastructure.

Accurics provides a fundamentally new approach for protecting cloud native infrastructure by embedding security during development to establish a secure posture and maintaining it through runtime. The Accurics platform detects and remediates policy violations as well as potential breach paths across Infrastructure as Code (IaC). It maintains the secure posture by monitoring cloud native infrastructure in runtime and assessing changes for risk. Developers are notified about legitimate changes and the code to update the IaC is checked into the repository for review. In contrast, developers are notified about risky changes and the code to revert to the secure baseline is provided so that they can reprovision the cloud and eliminate the change. Establishing IaC as the single source of truth for risk posture enables immutable security.




"As organizations embrace immutable infrastructure, manual changes to production cloud deployments will become untenable. The approach of governing infrastructure as code, and subsequently reconciling any posture drift between cloud deployments and code, will enable immutable security for immutable infrastructure."

— Krishna Bhagavathula, CTO @ NBA

# Use Cases

## Infrastructure as Code Security

Accurics connects to code repositories to scan Infrastructure as Code (IaC) such as Terraform, Kubernetes YML, Dockerfile, and OpenFaaS YML. It detects policy violations and identifies potential breach paths. Accurics also generates code to remediate issues and creates pull requests in the repositories. Developers simply need to review and merge the requests to resolve the issues.

## Cloud Security Posture Management

Accurics continuously monitors cloud infrastructure in runtime across AWS, Azure, and Google Cloud Platform environments and assess new resources and configuration changes for risk. It detects policy violations and identifies potential breach paths.

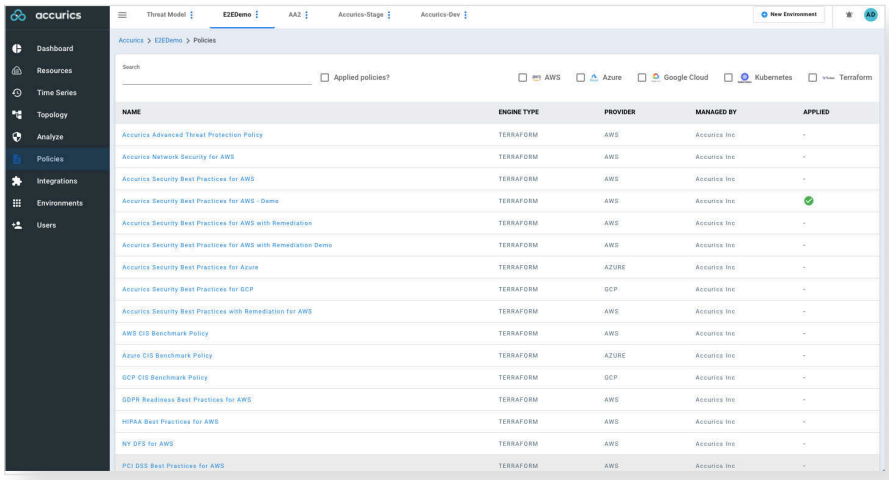
## Immutable Security

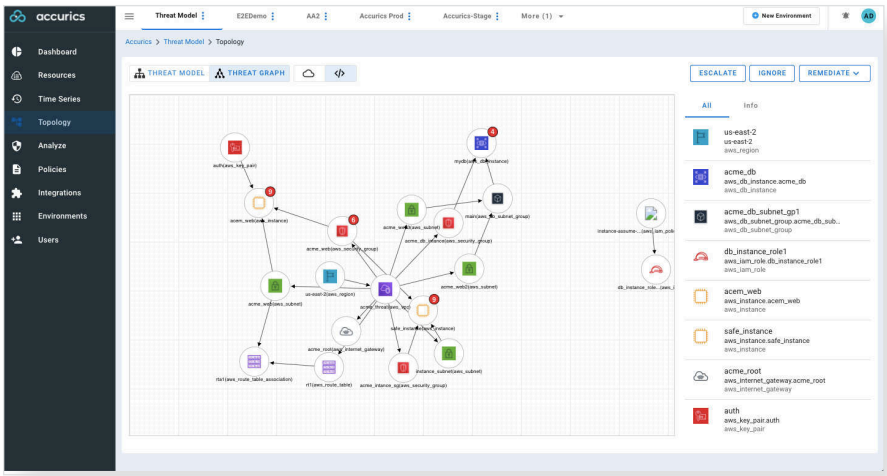
Accurics detects and remediates risks in IaC to establish a secure baseline from which cloud infrastructure is provisioned. It maintains the secure posture by monitoring cloud native infrastructure in runtime and assessing changes for risk. The IaC baseline is updated for legitimate changes; the cloud infrastructure is redeployed using the baseline to eliminate risky changes. Establishing the IaC as the single source of truth for risk posture enables immutable security.

# Product Features

## Policy as Code

As the scale and velocity of cloud adoption increases, policy guardrails to monitor cloud infrastructure definition and management becomes essential. Accurics provides 1500+ policies across 10+ standards such as CIS Benchmarks, SOC 2, PCI DSS, HIPAA, NYDFS, and GDPR so that policy guardrails can be enabled in minutes. Custom policies based on individual business needs can also be defined. During development, Accurics scans Infrastructure as Code (IaC) to detect policy violations. Accurics also integrates with CI/CD tools to detect violations and block risky builds. The same policies can be applied at runtime to continuously monitor cloud environments for risky changes.






## Security as Code

Aside from detecting policy violations, it is important to prioritize resolution of high severity risks. Accurics generates a real-time topology across all infrastructure by identifying resources, configurations, and dependencies between them. It then models threats against the topology using data such as threat feeds, trust boundaries, and IAM privileges to identify high severity issues. Accurics maps the threats to a killchain to determine if there are any breach paths and also analyzes the blast radius of a potential breach. This enables prioritization of high severity issues.

## Drift as Code

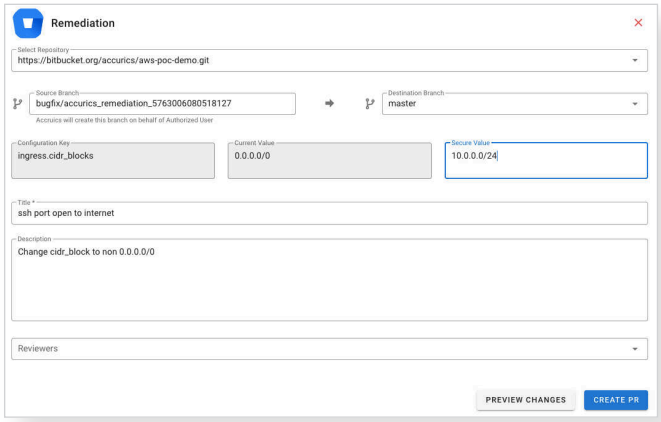
The constantly changing nature of cloud native infrastructure makes it necessary to continuously monitor for changes. Accurics enables organizations to establish a secure baseline through IaC or across cloud infrastructure in runtime. It then continuously monitors the cloud infrastructure to detect new resources and assesses them for risk. Accurics also monitors for configuration changes from the secure baseline and assesses for risk.

**Secure Baseline**

```
resource "security_group" "ssh" {
  ingress {
  cidr_blocks = [
  "10.0.0.0/24"
  ]
  to_port = 22
  }
}
```

**Configuration Change**

```
resource "security_group" "ssh" {
  ingress {
  cidr_blocks = [
  "0.0.0.0/0"
  ]
  to_port = 22
  }
}
```



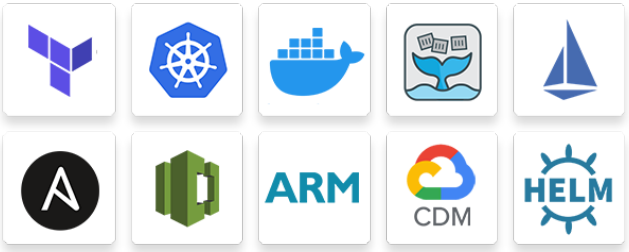

## Remediation as Code

Automatically detecting policy violations and threats across constantly changing cloud native infrastructure runs the risk of creating alert fatigue. In order to ensure that security does not hinder development, remediation workflows must be integrated into development pipelines. Accurics integrates with workflow tools such as Jira and Slack as well as code repositories such as GitHub, Bitbucket, and GitLab. When a policy violation occurs or a threat is detected, Accurics flags the issue and automatically generates code to resolve it. The code is checked into the repository as a pull request and the appropriate developer is sent a notification via Jira or Slack to review and merge the change. Optionally, the risky configuration can also be overridden in order to ensure that cloud infrastructure is provisioned securely.

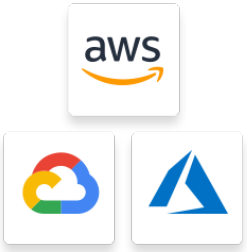
## Technologies You Can Secure

Secure your Infrastructure as Code during development and your deployed cloud native infrastructure in runtime.

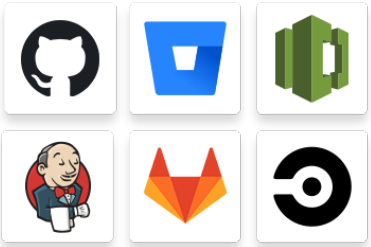
### Infrastructure as Code



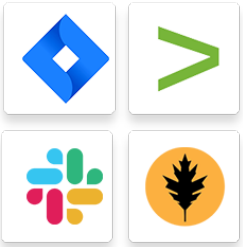

### Cloud Environments




### DevOps Tools



### Workflow Tools



## Works with Your Toolchain

Seamlessly connect Accurics with services in your development pipeline.

## Deployment Options

You can use Accurics as a cloud solution or download a self-hosted version to meet your organization's individual needs.

### SaaS

1. Get up and running in minutes with a fully managed instance
2. Alleviate the need for maintenance with automatic upgrades
3. Built with privacy by design principles

### Self-Hosted

1. Ensure data residency and sovereignty
2. Satisfy regulatory requirements
3. Complete private repository access

**Visit us at www.accurics.com to learn more**

accurics™