accurics™
Cloud Cyber Resilience™

Product Brief

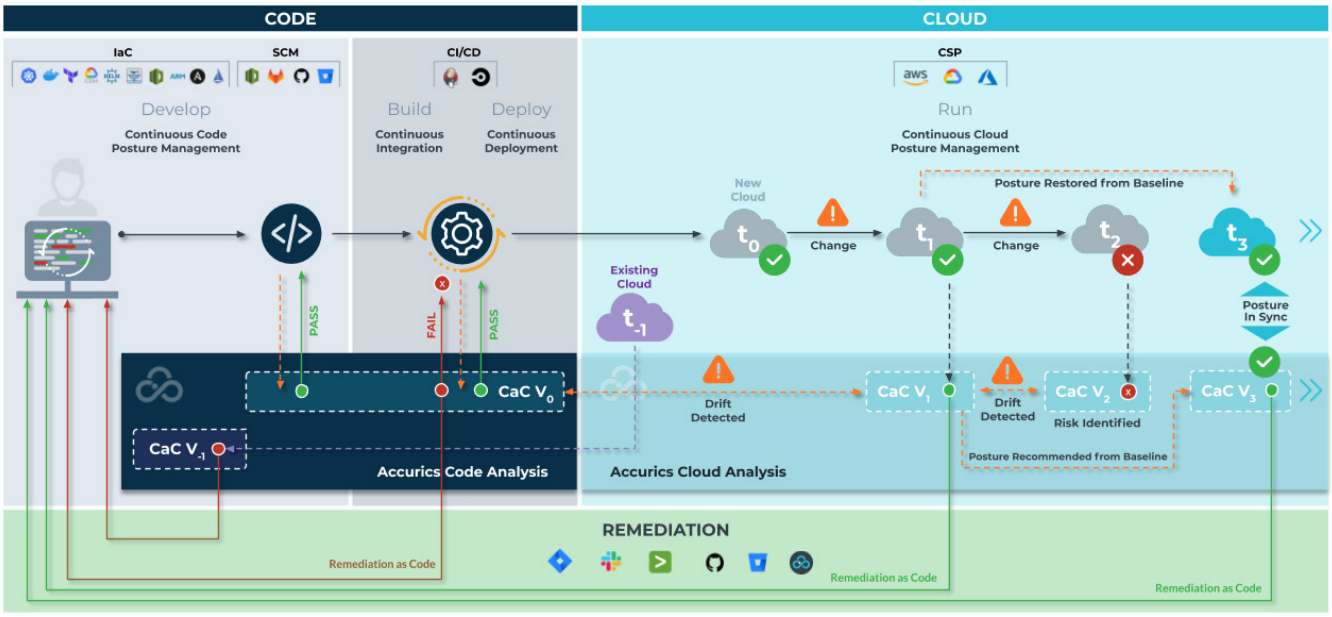
Self-Healing Cloud Infrastructure by Codifying Security

Cloud native technologies are fueling innovation and powering today's applications. Cyber resilience in the cloud is now more important than ever. However, cloud breaches are threatening innovation -- over 30 billion records have been exposed in 200 breaches over the last two years.

The unfortunate reality is that cloud breaches will continue to occur because development velocity is outpacing security velocity. Cloud native infrastructure is being programmatically defined through Infrastructure as Code (IaC), while risks are being mitigated manually. Cyber resilience can only be achieved through self-healing cloud native infrastructure.

Accurics codifies security throughout the development lifecycle to self-heal cloud native infrastructure. The Accurics platform programmatically detects and resolves risks across Infrastructure as Code (IaC) before infrastructure is provisioned and establishes a secure baseline. It monitors the cloud infrastructure in runtime against this baseline to detect changes to existing resource configurations or the creation of new resources, and assesses for risk. Developers are notified about non-risky 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.

Accurics Codifies Security Throughout the Development Lifecycle

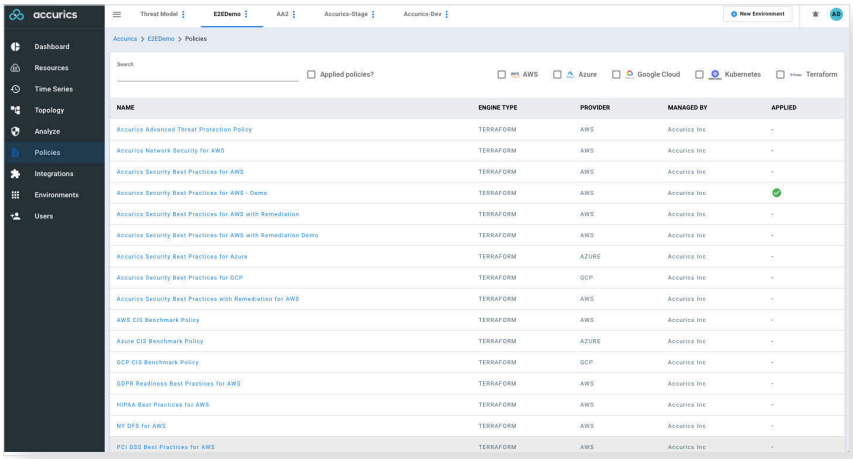


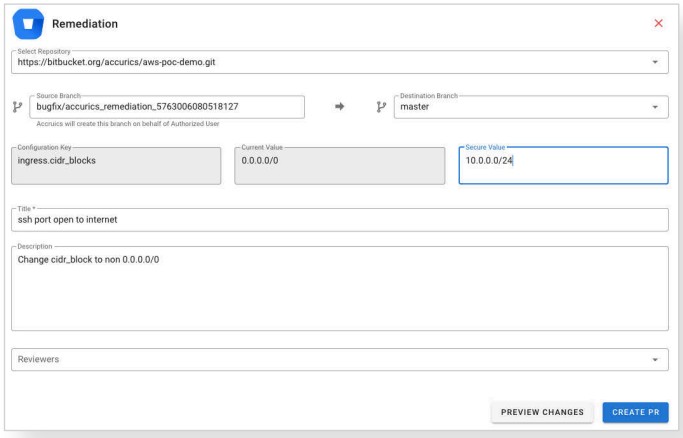
“As organizations embrace immutable infrastructure, manual changes to production cloud deployments will become untenable. The approach of governing infrastructure as code, and subsequently reconciling any posture drift between cloud deployments and code, will enable immutable security for immutable infrastructure.”

— Krishna Bhagavathula, CTO @ NBA

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 a library of 1800+ policies across common 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.





Remediation as Code

Automatically detecting issues 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 (self-healed) in order to ensure that the risk is eliminated before cloud infrastructure is provisioned securely.

Secure Baseline

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

Configuration Change

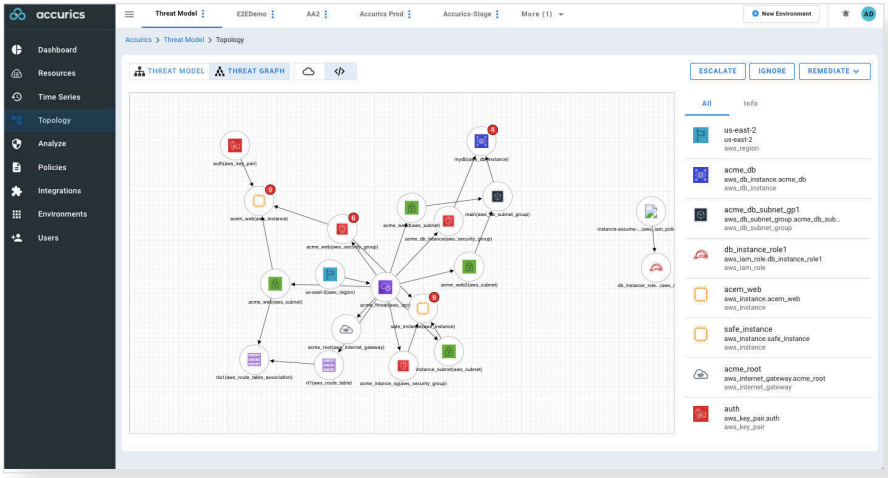
```
resource "security_group" "ssh" {
  ingress {
  cidr_blocks = [
  "0.0.0.0/0"
  ]
  to_port = 22
  }
}
```

Drift as Code

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

Security as Code

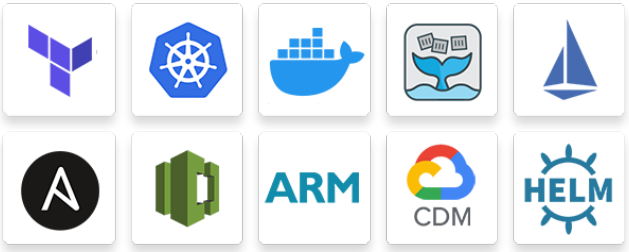
Aside from detecting policy violations, it is important to prioritize resolution of high severity risks. The Accurics platform generates a real-time topology across all infrastructure by identifying resources, configurations, and dependencies between them. It then models threats against the topology using data such as threat feeds, trust boundaries, and IAM privileges to identify high severity issues. The platform 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.



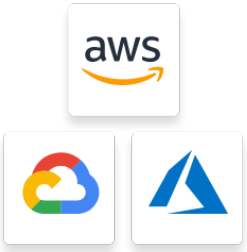
Technologies Accurics Can Secure

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

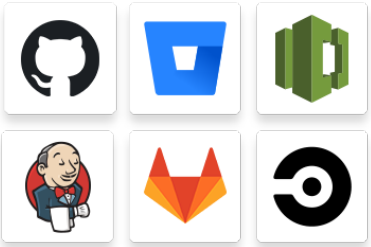
Infrastructure as Code



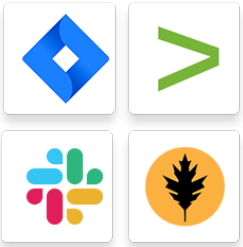
Cloud Environments



DevOps Tools



Workflow Tools



Integrations

Seamlessly connect Accurics with services in development pipelines.

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™