INFRASTRUCTURE-AS-CODE: CONNECTIVITY RISK ANALYSIS

Infrastructure-as-code (IaC) is a crucial part of DevSecOps practices. The current trend is based on the principle of shift-left which places security early in the development cycle. While security has multiple facets, AlgoSec focuses on application connectivity.

Incorporating secure application connectivity as part of your infrastructure-as-code allows organizations to take a proactive and preventive rather than reactive approach to secure application connectivity. Developers often leave security checks and testing for later stages of a project, often as it nears completion and deployment. It is a well- known that the costs of fixing an error in production are much higher than fixing it in code. To promote a preventive approach to secure application connectivity, we need to align people, processes, and technology.

Key challenges of a preventive security approach

- Manual security scanning is a time-consuming, process that often results in human errors and bottlenecks in delivery
- Risk analysis not built into the development process
- Static, non-customizable connectivity risk analysis results in numerous false positives
- Multiple stakeholder workflows from risk discovery and analysis to remediation

Key benefits

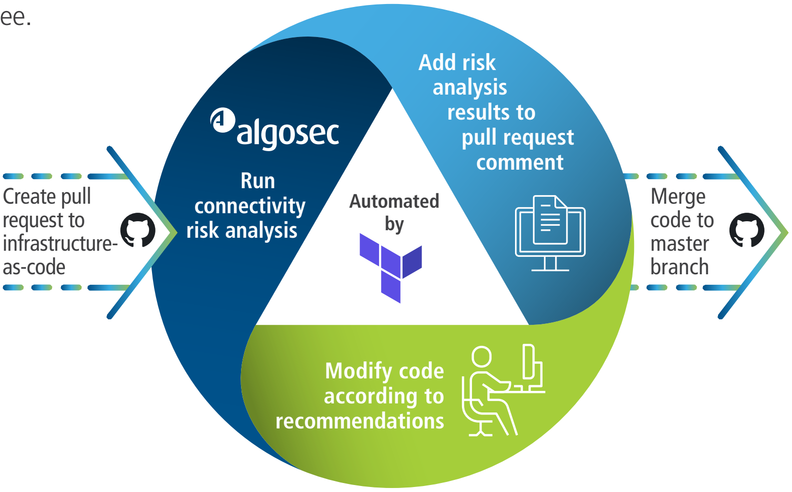
- Deliver business applications into production faster and more securely
- Enable a frictionless workflow with continuous risk analysis and remediation
- Reduce connectivity risks earlier in the CI/CD process
- Customizable risk policy to surface only the most critical risks

AlgoSec's IaC solution

AlgoSec's IaC solution is an extensible security plugin platform that checks code for potential vulnerabilities before any commits are made to a repository. Accelerate application delivery taking a proactive, preventive, and collaborative approach within your CI/CD pipeline. Developers have clear visibility into risks right in the source control applications and are given clear remediation steps without a need to move to different applications or wait for security admin to manually review and approve that the code is risk free.

Figure 1: Proactive risk analysis

Gain a comprehensive risk analysis as part of the pull request. The analysis identifies all critical connectivity related security risks defined by the customer in their risk policy. The developer receives recommendations for remediation ensuring swift resolution.


Create pull request to infrastructure-as-code
algosec
Run connectivity risk analysis
Add risk analysis results to pull request comment
Automated by
Modify code according to recommendations
Merge code to master branch

algosec | SECURELY ACCELERATE

AlgoSec.com

Copyright © AlgoSec Inc. All rights reserved. AlgoSec is a registered trademark of AlgoSec Inc.
The AlgoSec Logo is a trademark of AlgoSec Inc. All other trademarks used herein are the property of their respective owners.