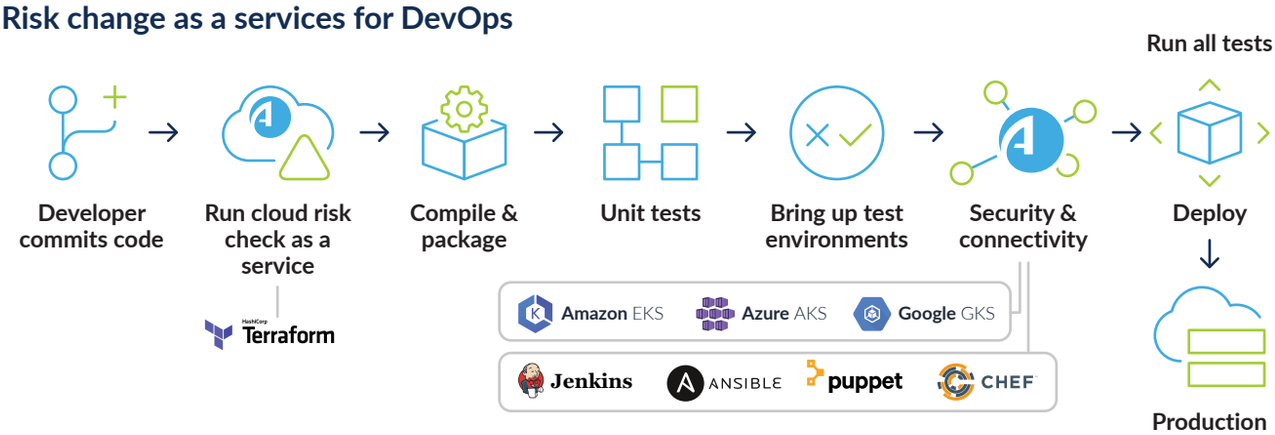
algosec

Secure application connectivity.
Anywhere.

Optimizing DevOps
Flawlesly hit your delivery target

Proactively identify risk early in the development processes, perform connectivity status check and automatically implement connectivity changes if needed.

Risk change as a services for DevOps



Key pain points in securing your CI/CD pipeline

1. Delays in development and deployment due to security reviews and code fixes
2. Connectivity issues leading to extended troubleshooting and deployment delays
3. Challenges in meeting compliance requirements in fast-paced DevOps environments
4. Supply chain malware and vulnerabilities entering production

DevOps methodology revolutionizes the speed of bringing business applications to market, allowing organizations to be more agile and keep up with the demands. At the same time, the traditional approach of addressing security concerns late in the development process causes delays and additional burdens for DevOps teams.

To bridge this gap, it is essential to incorporate security into the DevOps workflow from the beginning. By integrating security into the development lifecycle, you can take a proactive and efficient approach to prevent delays and mitigate security risks. This approach enables DevOps teams to prioritize fast and high-quality application delivery while maintaining a strong focus on security.

Streamline security, compliance, and faster deployments

By Integrating the AlgoSec platform into your current DevOps tools, you can effectively facilitate the complete DevOps lifecycle and synchronize security measures with build, QA, and deployment procedures. This collaborative integration from the outset strengthens security and compliance, effectively eliminating delays in security fixes. By giving priority to security, you establish trust with stakeholders and regulatory bodies, ultimately reducing time-to-market and driving operational excellence.

Speed up application delivery without compromising security

AlgoSec's IaC (Infrastructure as Code) connectivity risk analysis helps DevOps teams accelerate application delivery and optimize security. Developers can proactively check for vulnerabilities using this powerful capability before pushing code to a repository.

By using source control apps, you can eliminate manual security reviews and empower your team to respond quickly by following clear remediation steps. Improve security, enhance efficiency, and achieve DevOps excellence by utilizing IaC connectivity risk analysis.

Empower your DevOps workflow with seamless connectivity integration

The seamless integration between AlgoSec and Chef, Puppet, and Ansible enables application developers to easily define network connectivity. Application connectivity requirements can be conveniently specified in a straightforward file without diving into network infrastructure details, offering numerous advantages by describing them as logical flows.

By translating these requirements into firewall rules, AlgoSec's solution streamlines development and reduces delivery costs. With zero-touch, easily update connectivity requirements.

Lock down container security with smart threat management

AlgoSec threat management scan & secure your containers in real-time, blocks risky connections, malware, and vulnerabilities while empowering you to customize control through block/allowlists and set automated mitigation based on defined risk levels, all seamlessly integrated with GitHub and AWS ECR pipelines.

algosec

AlgoSec.com