algosec

INTEGRATE SECURITY INTO DEVOPS FOR FASTER, SAFER APPLICATION DELIVERY INTO PRODUCTION

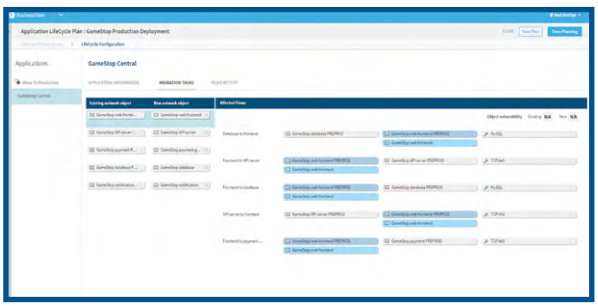
The DevOps methodology enables companies to deliver innovations faster to market. Automation is incorporated into this framework to speed up the process of deploying applications and their supporting infrastructure — servers, storage, and networking — throughout the development lifecycle. However, with multiple functional teams collaborating on development, and so many moving parts, the security team is often left out of the DevOps process. As a result, security management is tacked on at the end and it can take up to three weeks to provision new network connectivity — which ultimately negates many of the benefits of DevOps and delays deployment into production.

Key challenges of incorporating security into the DevOps process include:

- Aligning the security and network operations teams and processes with developers' deployment requirements
- Identifying each business application's network connectivity requirements, before deployment
- Managing the deployment of network security throughout development, QA and production
- Manual and error-prone security change management processes
- Ensuring regulatory and corporate compliance

AlgoSec Security Policy Management for DevOps

Through its application-centric approach, AlgoSec extends automated security policy management into existing DevOps practices and tools and supports the entire DevOps lifecycle — from build, through QA, to deployment into production. This allows for better collaboration between security and the DevOps teams right from the start, and enables faster deployment into production while ensuring that the development and production environments are secure and compliant at all times.



Key Benefits

- Align security, networking, and application teams, and foster DevOps
- Automatically identify existing applications and their connectivity flows – without requiring coding or prior knowledge
- Define and provision network security throughout the DevOps lifecycle and into production
- Automate the entire network security change management process
- Ensure security and compliance throughout the DevOps process

CHEF

puppet

ANSIBLE

Easily Define and Deploy Network Connectivity Throughout the DevOps Lifecycle

AlgoSec integrates with the leading CI tools, including Chef, Puppet and Ansible, to empower application developers to define network connectivity as an integral part of their application coding process.

With AlgoSec, the application developer can specify the application connectivity requirements needed, as a list of logical flows, in a simple file. No additional details about the network infrastructure, firewalls, etc. are needed. Once the list is created, the AlgoSec Security Management Solution automatically translates these requirements into the necessary firewall rule changes and implements them — without needing any additional inputs from the developer. Whenever a new version of the application is developed, the developer simply updates the list of connectivity requirements, and AlgoSec then provisions any necessary changes — all with zero touch.

Automatically Discover Existing Applications' Network Connectivity to Establish a Baseline

Integrating network security into the DevOps process requires an initial mapping of the existing network network connectivity flows. Not only does the connectivity map help expedite the security policy change process throughout the DevOps lifecycle, it also helps establish a common language between the network-centric security teams and application-centric DevOps teams, making it far easier to facilitate collaboration throughout the DevOps process.

AlgoSec automatically discovers and maps the network connectivity flows between business applications and servers to provide the necessary baseline to help accurately plan and deploy network security changes.

Proactively Assess Risk Throughout the DevOps Process

With every change process, AlgoSec automatically and proactively assesses all changes for risk and compliance. This enables the security team to uncover and address any problems before any changes are made — thereby ensuring the integrity of the security policy while maintaining continuous compliance with industry regulations.

Maintain Network Security in Production

In production, AlgoSec automatically manages the security policy across the entire enterprise environment — in the cloud, across SDN and on-premise networks — on an ongoing basis.

With AlgoSec users can:

- Get full visibility across the entire enterprise environment in a single pane of glass
- Automate security policies changes and prevent misconfigurations
- Proactively assess risk to detect unauthorized or risky changes, and ensure compliance
- Safely clean up and optimize inefficient or unnecessary firewall and router policies
- Automatically generate compliance reports for all regulatory standards and corporate policies

Self-Service Security Policy Management with AlgoBot

Developers can also manage network security changes through AlgoSec's AlgoBot, an intelligent chatbot that handles day-to-day network security policy management tasks. With AlgoBot, developers can get answers to network connectivity questions immediately, and request security policy changes—without requiring manual inputs, additional research, or having to track down the firewall administrator.

AlgoBot can:

- Check if traffic is currently allowed between IP addresses, servers and applications
- Check if a business application has a network connectivity problem
- Open change requests to allow network connectivity
- Check on the status of a change request
- Identify all applications associated with a specific IP address

algosec

AlgoSec.com