PROTECTING KUBERNETES CLUSTERS IN AWS AND AZURE

Kubernetes computing services such as Amazon Elastic Kubernetes Service (Amazon EKS) and Azure Kubernetes Service (AKS) have become extremely popular as organizations scale up and adopt lightweight application deployment methodologies.

However, the rapid adoption of Kubernetes computing services creates challenges for organizations looking to obtain visibility and assess security risks across their cloud deployments.

Gain visibility into your Kubernetes entry points and mitigate risks

Complete visibility: You can't protect what you can't see

Full visibility is essential to avoid security breaches at the entry point to your Kubernetes nodes and pods. AlgoSec makes the security measures in place, visible at all entry or exit points to your Kubernetes environments. These entry and exit points either direct inbound traffic from the Internet (Public IPs) and Internal Networks (Private IPs), or direct outbound traffic to the Internet from the Internal Networks.

Visibility into the security rules governing the Kubernetes services ensures that an organization can detect over-permissive permissions and vulnerabilities. As a result, security breaches can be minimized.

Risk Analysis

AlgoSec can be used to run an ongoing risk analysis of the Kubernetes services to prevent network breaches. For example, customers that expose their Kubernetes nodes to the Internet with an "any" source and an "any" service in their security group rules are placing their Kubernetes nodes at risk. Identifying and mitigating such risks minimizes the chances of a network breach.