Alcide Kubernetes Security

Help protect Amazon EKS deployments

Why Alcide?

- **Deep visualization** – Alcide provides a visual map with real-time mapping of the entire environment helping you troubleshoot and mitigate security issues.
- **Enforcement and threat detection** – Alcide machine learning algorithms help ensure your infrastructure, policies, and network activities stay safe and compliant in real time.
- **Extending AWS security group policies** – Automatically import AWS workload security groups to gain more granular policy segmentation control, display all policy data, and enhance protection against security events.

Product overview

With a speedy integration for AWS, Alcide helps DevSecOps leverage Amazon Elastic Kubernetes Service (EKS) to secure Kubernetes deployments at scale. Updating as workloads spin up and down, Alcide quickly identifies security events and alerts on non-compliant and anomalous behavior. With a centralized dashboard and graphical network map, you can view a broad picture of all activity to troubleshoot and mitigate issues in real-time. Alcide guides you in implementing native AWS guardrails and adopting and monitoring your own security policy model. You can also gain granular control by importing all workload security groups and policy data to protect dynamic deployments with in-context metadata and visibility.

Product features

Automate security and configuration checks already from development

The Alcide Advisor automatically and continuously scans and checks security and configuration posture, helping you resolve security issues in the development stage. The Advisor audits the cluster, node, and pod configurations to ensure the cluster is tuned and runs according to best practices and internal guidelines. While doing so, it provides actionable mitigation recommendations. This includes cases such as image registry whitelisting, workload and pod segregation, identity and access management (IAM) and role-based access control (RBAC) policies, and more.

Real-time automated monitoring of policies and threat detection

Alcide Runtime consolidates all AWS security groups, policies and corresponding inbound and outbound rules across networks in one dashboard, helping enforce application-aware embedded policies for cloud infrastructures and microservices. Alcide also provides threat detection that includes abnormal behavior and incident monitoring. Respond to anomalies in real-time with security-tuned machine learning that helps identify unusual patterns, network usage, and data transfers.

Solution available in AWS Marketplace