ALCIDE KUBERNETES SECURITY

Secure Kubernetes & Service Mesh. Anywhere.
Bridging Security & DevOps.

COMPANY DESCRIPTION

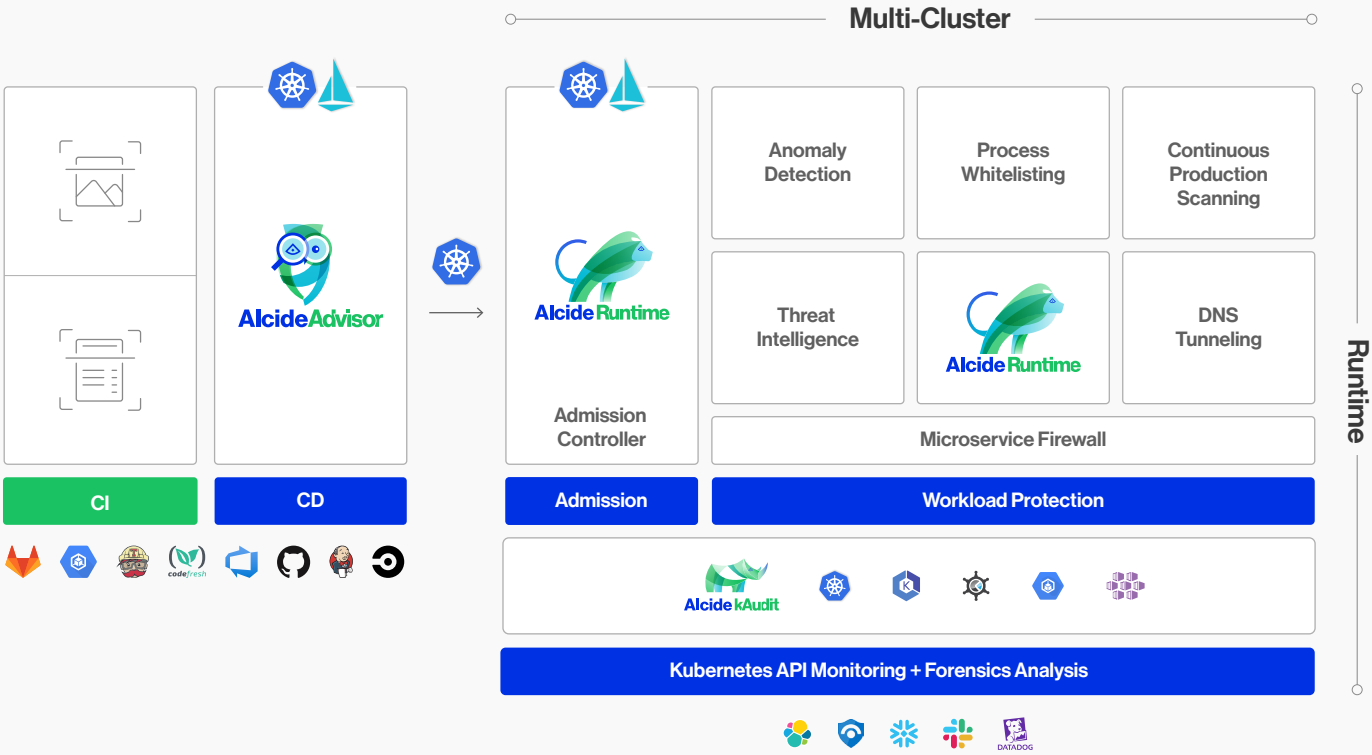
Alcide is a Kubernetes security leader empowering DevOps teams to drive frictionless security guardrails to their CI/CD pipelines, and security teams to continuously secure and protect their growing Kubernetes deployments. Alcide provides a single Kubernetes-native and AI-driven security platform for cross Kubernetes aspects: configuration risks, visibility across clusters, k8s control plan, detecting insider threat, compliance monitoring and run-time security events. Combined with policy enforcement, and a behavioral anomaly engine that detects anomalous and malicious network activity, Alcide ensures that the entire Dev. to production pipeline is secured.

ALCIDE KUBERNETES AND ISTIO SECURITY PLATFORM

- Deep visibility into Kubernetes and Istio network and hygiene
- Software supply chain misconfiguration drift
- Cluster hardening: vulnerability scans and compliance checks
- Threat intelligence
- Kubernetes insider threat detection
- Automation and observability for rapid deployments

PRODUCT DESCRIPTION

Alcide helps organizations speed and automate deployment by enforcing configuration drifts and security policies during the build stage. It maintains continuous Kubernetes and Istio cluster hygiene by automatically applying best practices, vulnerability scans and compliance checks. At Runtime Alcide applies workload segmentation and network anomalies detection to prevent data or network breaches as they happen. Alcide provides near real-time Kubernetes API monitoring and forensic analysis to detect K8s-related breaches, anomalous behavior or misuses using K8s audit logs.



ALCIDE USE CASES

K8s Security Assurance from CI/CD Pipeline

Visibility for misconfig and risks, Cluster hygiene, Policy recommendation and enforcement (Fail build)

Audit & Monitoring

Detect security-related abuse and abnormal behaviour monitoring via the Kubernetes audit log analysis.

Compliance in Kubernetes

Providing best practice configuration validation, microsegmentation, malware protection, deep visibility and monitoring capabilities.

Kubernetes Security for the Edge

Balance security between the Edge core and the Cloud core.

Cloud Micro-segmentation

Prevent data breach using workload segmentation.

Threat Detection

Protection against multiple attack vectors: abnormal behavior and security incidents such as DNS exfiltration, spoofing, poisoning, and lateral movement.

Superior Visibility

Providing visibility across multi-cluster environments.

WHY ALCIDE

Tailored for Kubernetes and Istio

Using native Kubernetes capabilities providing policy-driven Kubernetes scans, automatic updates, and network and control plane policies enforcement.

DevOps, SecOps first approach

Embedding dev, and devops know-how continuously with an active and dynamic analysis of network, permissions and configurations.

Network Security DNA

Alcide Threat Detection engine analyzes network traffic and leverages Machine Learning (patent pending) algorithm to detect behavior anomalies and security incidents.

In-Depth Visibility & Observability

Centralized view for the entire Kubernetes stack: showing interdependencies between the network and applications, and expose potential risks.

Detection of Known & Unknown K8s Threats on NW and Control Plan Traffic

Applying NW segregation and access list policies as well identifying threats based on threat intel. database. Identifying K8s network and control plane abuse based on patent-pending AI.