alcide

Microsoft Azure

Certified

Securing AKS Deployment with Alcide Kubernetes Security Platform

Enforcing Kubernetes security best practices are major bottlenecks to implementation and deployment

Cloud-native technologies are new and evolving fast, and a key part of a company's success depends on the security teams' ability to monitor and operate digital services and assets in the most reliable way.
As enterprises are adopting Kubernetes into production, more and more security challenges pop up when managing one or more clusters across different hosts, which ultimately slows down operation cycles.
With the rise of Kubernetes as a de facto standard tool for managing all application workloads,there is also a correlated increase in attack surfaces and security risks that must be taken under consideration.

Alcide helps secure and ensure Kubernetes multi-cluster hygiene

Alcide's native security solution for Microsoft Azure Kubernetes Services (AKS) provides cloud discovery, deep visibility into the entire cloud topology, and application data flow with ongoing security and hygiene checks that alert on security and misconfiguration drifts.
Combined with Alcide behavioral anomaly threat engine that detects anomalous and malicious network activity, Alcide ensures that the entire dev to production AKS pipeline is secured.
The integration process is swift and brings organizations the ability to have a faster identification of specific Ops and security issues, track back to responsible parties, and troubleshoot and identify root cause with ease.

Benefits

Integrate security checks as early as your CI/CD workflow, securing multi-cloud and hybrid deployments, and visualize changes as they happen. Manage workloads granularly, enforce compliance and ensure remediation is performed on time.

Deep visualization

Automatically import Azure security groups and policies from all of your networks, enabling granular control of policy segmentation, displaying all policy data, and protecting against threats.

Extending Microsoft security & access features

Alcide helps developers configure build-time security rules for Azure services and external DNS names, and provides a real-time visual map of your entire environment helping to troubleshoot and mitigate security issues.

Enforcement and real-time threat detection

Alcide detects pod-level network activity with crypto-mining, command and control, drop location, and more. Our machine learning algorithms help ensure infrastructure, policies and network activities stay safe and compliant.

Continuously protect multi-cloud environments

Alcide continuously discovers and manages policies with code-to-production enforcement across all your networks, empowering DevSecOps teams to scale multi-cluster deployment security.

alcide

Alcide on Microsoft Azure Kubernetes Service & DevOps

Alcide kAudit

A real-time, automated AI-driven security platform for forensics and analysis of Kubernetes audit logs

Alcide kAudit is designed to automatically analyze Kubernetes audit logs in and is seamlessly integrates with Azure Sentinel.
kAudit automatically detects security-related issues related to Kubernetes' administrative actions, especially anomalous behavior that can only be spotted from observing extended context over multiple activities.

Furthermore, kAudit supports Audit rules to detect violations of organization compliance policies regarding Kubernetes usage. Incident forensics, along with audit statistics, are presented in graphical and tabular summaries for easy investigation and analysis.

Get started with Alcide solutions on Microsoft

Visit Microsoft Azure Marketplace or Alcide.io to purchase or start a Free Trial today.

www.alcide.io • info@alcide.io