



Ensure Kubernetes Security, Compliance, and Operational readiness for Amazon Web Services with Nirmata

Nirmata for Amazon EKS, EKS-D, and EKS Anywhere

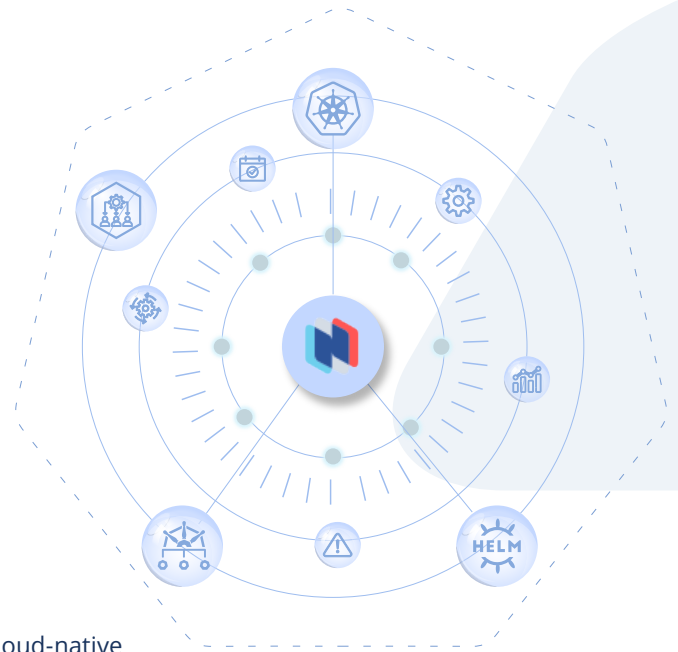
Today, organizations of all sizes and across all industries are adopting cloud-native technologies to take advantage of the agility, flexibility, and resilience they offer. Containers have become the de-facto way to package applications, and Kubernetes is the orchestration platform of choice. As the adoption of Kubernetes grows, enterprises often run into challenges when trying to securely scale and automate their Kubernetes infrastructure across regions, teams and for multiple applications. Nirmata provides centralized management and governance for Amazon EKS, enabling enterprises to accelerate their cloud-native journey without requiring significant expertise and resources.

Challenge

As enterprises embark on their cloud-native journey, their progress is often stalled due to the operational complexity and security risks caused due to the growing infrastructure. Although Kubernetes is extremely powerful and versatile, the configuration and operation of these environments quickly becomes difficult to manage and scale. Additionally, scaling Kubernetes requires expertise and coordination across developers, operations, and security teams.

Securing the Kubernetes infrastructure without compromising on developer agility holds the key to success with cloud-native adoption. Some of the challenges that enterprises need to overcome when scaling Kubernetes include:

- Lack of central visibility for their clusters and applications that are deployed across regions and accounts.
- Lack of governance introduces significant risks especially when sharing clusters between teams and applications.
- Complexities associated with ensuring that security and compliance standards are met.
- Possibility of compromising the security posture of the cluster and workload due to misconfigurations and lack of image verification controls.
- Loss of productivity because of ongoing back and forth between development, security and operations teams when identifying, troubleshooting, and addressing security issues.
- Reduced developer agility due manual handoffs and the inability to get on-demand access to cluster resources, in a secure manner.



Why Nirmata for AWS

- Centralized management and governance for Amazon Elastic Kubernetes Service (EKS), Elastic Kubernetes Service Distro (EKS-D) and Elastic Kubernetes Service Anywhere (EKS Anywhere).
- Enabling enterprises to effortlessly adopt Kubernetes and operate it at scale.
- Nirmata uses a policy-driven approach, powered by Kyverno, the Kubernetes native policy engine, for governance, automation, security, and compliance with AWS.



Solution

Nirmata DevSecOps Platform is a turnkey, application-centric platform that simplifies operations and governance of Amazon EKS clusters and workloads. Nirmata DevSecOps Platform is available in the AWS Marketplace.

Kubernetes Management and Governance Built for AWS:

Nirmata DevSecOps Platform delivers centralized visibility, management, security, and governance of Amazon EKS clusters. With Nirmata, enterprises can rapidly and securely scale the adoption of Amazon EKS across teams and applications while enabling developer agility and cross team collaboration.



How Nirmata DevSecOps Platform works

Nirmata DevSecOps Platform is purpose-built to allow enterprises to leverage Amazon EKS, EKS-D and EKS Anywhere at scale. Nirmata delivers these capabilities:

Self-service deployment: Unleash developer agility by providing self-service access to clusters with the requisite security: a secure host OS, policy engine for governance and compliance, and possibly other runtime security tools. Allow users to override certain configurations such as instance types or instance counts while ensuring that other complex configurations for network, security, logging etc. are not modifiable.

Secure access to clusters and AWS services: Provide granular access to clusters and namespaces across the entire fleet of clusters independent of the location and how they are deployed. Automatically configure IAM roles for service accounts to ensure only specific workloads can access AWS services.



Learn More

Policy-driven management and governance: Define a set of rules created through policies that are enforced on all clusters to ensure best practices are adopted. Ensure clusters can be securely shared across teams and applications. Automatically generate Kubernetes resources based on certain triggers such as labels and annotations to configure necessary guardrails and automate workflows.

Continuous security and compliance: Automatically monitor and ensure security and configuration controls to meet industry compliance standards such as CIS and NIST 800-53 or corporate standards. Ensure only signed and attested container images are deployed on your clusters reducing the risk of software supply chain attacks.

Progressive delivery of applications: Automate the delivery of your applications using GitOps. Enable progressive delivery for multi-cluster deployments and get complete visibility into the status of your rollouts.

Comprehensive resource visibility: Centrally view and manage clusters across regions and accounts to better understand and optimize workloads and resources as well as troubleshoot issues. Get instant visibility into resource utilization, availability, state, and cost.

Easy integration with DevOps tools: Promote collaboration between development, security and operations teams through automated workflows and integrations with tools. Forward alarms and notifications to Slack, email or create Jira tickets.

Zero lock-in: Eliminate any vendor lock-in for your Kubernetes infrastructure. Nirmata is an out-of-band management system that allows you to add/remove clusters as needed without any impact to your workloads.

Working with Nirmata and AWS allows us to avoid DevOps bottlenecks without compromising security. We can set the right security policies to ensure the cluster is unaffected.

It keeps our day clean, improves productivity, and we can sleep better at night."

– KRISHNA BOPANA
DIGITAL MEDIA SOLUTIONS,
HEAD OF TECHNOLOGY
IQVIA

[ACCESS THE CASE STUDY HERE](#)

HIGHLIGHTED CUSTOMERS



About Nirmata

Nirmata, the creators of Kyverno, a CNCF Kubernetes native policy engine, provides open source and commercial enterprise solutions for governance, compliance, security, and automation of Kubernetes clusters and workloads. Nirmata enables secure, self-service cluster provisioning, provides DevOps teams visibility, health, metrics, and alerts, ensures security, compliance, and governance via workload policies, and streamlines application, and deployments across Kubernetes clusters deployed on any cloud, data center, or edge.



[Learn More](#)