nirmata
the creators of Kyverno

Nirmata Control Hub

Automate Security & Operations with Policy as Code

Introduction

Nirmata Control Hub offers a unified solution for policy-based security, compliance, and automation. Nirmata Control Hub provides central visibility, automated remediation, collaboration workflows, and continuous compliance for Infrastructure as Code (IaC), Kubernetes clusters, and Cloud Services. Using Control Hub, platform engineering teams can reduce the time taken to fix security issues and ensure clean production environments.

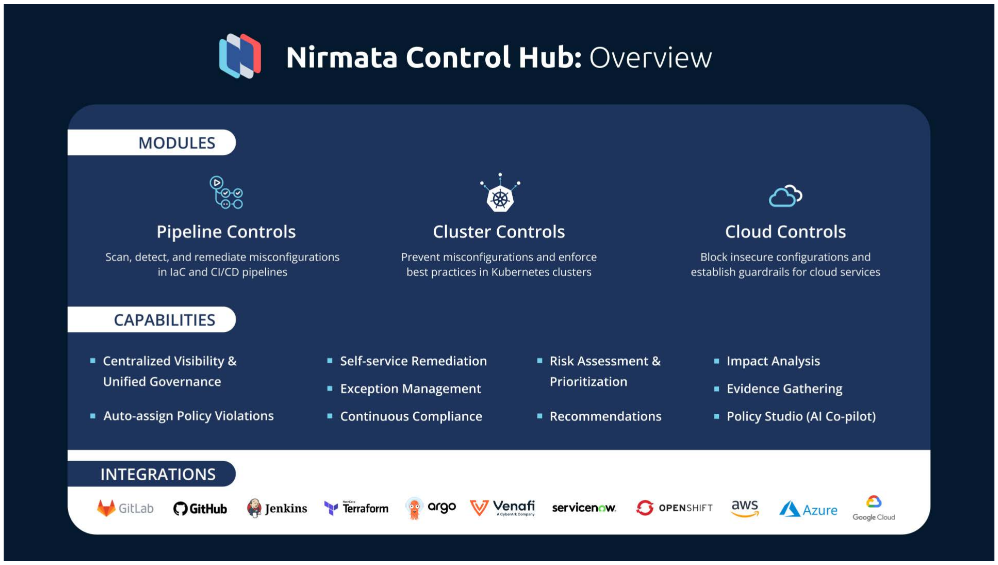
Enforce best practices and compliance, securing cloud-native applications by preventing misconfigurations

Simplify operations using a broad range of security, automation and best practice policies

Promote ongoing compliance and early issue detection via integration with DevOps tools

Key Benefits

- **Policy enforcement:** Proactively prevent misconfigurations and security issues by enforcing security best practices, community crowdsourced or custom-developed policies.
- **Policy-as-Code:** Easily manage policies through their entire lifecycle, ensuring consistent deployment and governance.
- **Central Visibility:** Gain insights on the effectiveness of policy through reporting and contextual correlation and insight engine.
- **Continuous Compliance:** Protect software supply chain with continuous compliance through policies as a standard part of DevOps pipeline.
- **Exception Management:** Streamline policy exception management for fine-grained control and compliance
- **Remediation:** Get actionable suggestions for addressing cluster violations, ensuring robust security and compliance
- **Collaboration:** Leverage existing processes and workflows through integrating with tools like Git, Slack, Jira and others.



Nirmata Control Hub: Overview

MODULES

Pipeline Controls
Scan, detect, and remediate misconfigurations in IaC and CI/CD pipelines

Cluster Controls
Prevent misconfigurations and enforce best practices in Kubernetes clusters

Cloud Controls
Block insecure configurations and establish guardrails for cloud services

CAPABILITIES

- Centralized Visibility & Unified Governance
- Auto-assign Policy Violations
- Self-service Remediation
- Exception Management
- Continuous Compliance
- Risk Assessment & Prioritization
- Recommendations
- Impact Analysis
- Evidence Gathering
- Policy Studio (AI Co-pilot)

INTEGRATIONS

GitLab GitHub Jenkins Terraform argo Venafi servicenow OPENSHIFT aws Azure Google Cloud

TRY NIRMATA CONTROL HUB

Key Features

- Centralized visibility for Security and Governance
- Automated policy distribution across clusters.
- Intelligent Policy to Cluster and Workload mappings.
- Continuous security and compliance throughout the development process.
- Streamlined policy exception management for fine-grained control.
- Automated remediation suggestions for addressing violations across clusters
- Rich Integration with DevOps workflows and tools to create alerts, tickets, and notifications

Use Cases

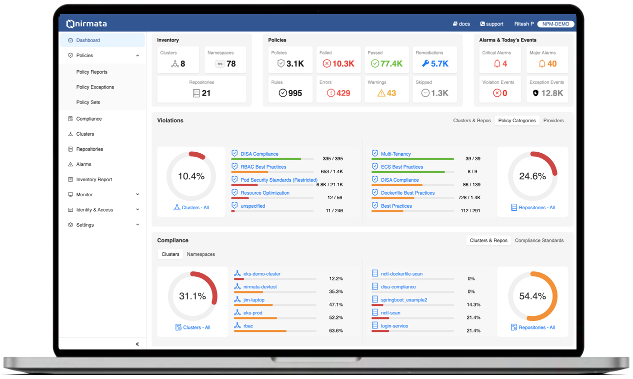
- **Eliminate Security Issues and Misconfigurations**
  Nirmata Control Hub eliminates security issues and misconfigurations by providing a cloud native, declarative policy-as-code solution for policy enforcement using Kyverno and an extensive collection of policies. It combines commercial policy lifecycle management solution that includes Policy Violation Alerts, Insights and Reporting, Developer Self-service, Secure and Automated Policy Distribution, a robust set of curated best practices policy and DevSecOps Process Automation and Integrations.

- **Shift Security Down**
  The Nirmata Control Hub integrates with build tools to provide visibility into policy violations and best practice recommendations. With Nirmata Control Hub you can facilitate effective and efficient DevSecOps and achieve cloud native agility without sacrificing security and governance.

- **Simplify Remediation**
  Nirmata Control Hub offers actionable suggestions for remediating violations. When it detects violations or deviations from defined policies, it doesn't just stop at alerting you – it goes a step further by providing actionable suggestions for remediation. This proactive approach streamlines the process of resolving issues and maintaining the desired state of your clusters, ultimately saving time and ensuring that your infrastructure remains secure and compliant.

- **Promote Agility with Collaboration**
  Nirmata Control Hub works the way that DevOps teams want to by letting organizations realize the true value of DevSecOps for Cloud Native environments. It leverages existing processes and workflows through integrating with tools like Git, Slack, Jira, and others.

- **Secure Software Supply Chain**
  Nirmata Control Hub enhances software supply chain security by mandating the use of images from trusted sources only. You can enforce policies to ensure that only cryptographically signed images are permitted to run, reducing the risk of tampered images.



Inventory

Clusters 8
Namespaces 78
Repositories 21

Policies

Policies 3.1K
Failed 10.3K
Passed 77.4K
Remediations 5.7K
Rules 995
Errors 429
Warnings 43
Skipped 1.3K

Alarms & Today's Events

Critical Alarms 4
Major Alarms 40
Violation Events 0
Exception Events 12.8K

Violations

10.4%
Clusters - All

DISA Compliance 335 / 395
RBAC Best Practices 653 / 1.4K
Pod Security Standards (Restricted) 6.8K / 21.1K
Resource Optimization 12 / 56
unspecified 11 / 246

Multi-Tenancy 39 / 39
ECS Best Practices 8 / 9
DISA Compliance 86 / 139
Dockerfile Best Practices 728 / 1.4K
Best Practices 112 / 291

24.6%
Repositories - All

Compliance

31.1%
Clusters - All

eks-demo-cluster 12.2%
nirmata-devtest 35.3%
jim-laptop 47.1%
eks-prod 52.2%
rbac 63.6%

nctl-dockerfile-scan 0%
disa-compliance 0%
springboot_example2 14.3%
nctl-scan 21.4%
login-service 21.4%

54.4%
Repositories - All

Nirmata is a proud member of the Kubernetes community

Nirmata is a leading policy-as-code platform that simplifies and automates security, governance, and compliance for Kubernetes and cloud-native environments. Powered by Kyverno, Nirmata enables real-time policy enforcement across multi-cloud and hybrid infrastructures, ensuring secure and compliant operations at scale.

TRY NIRMATA CONTROL HUB