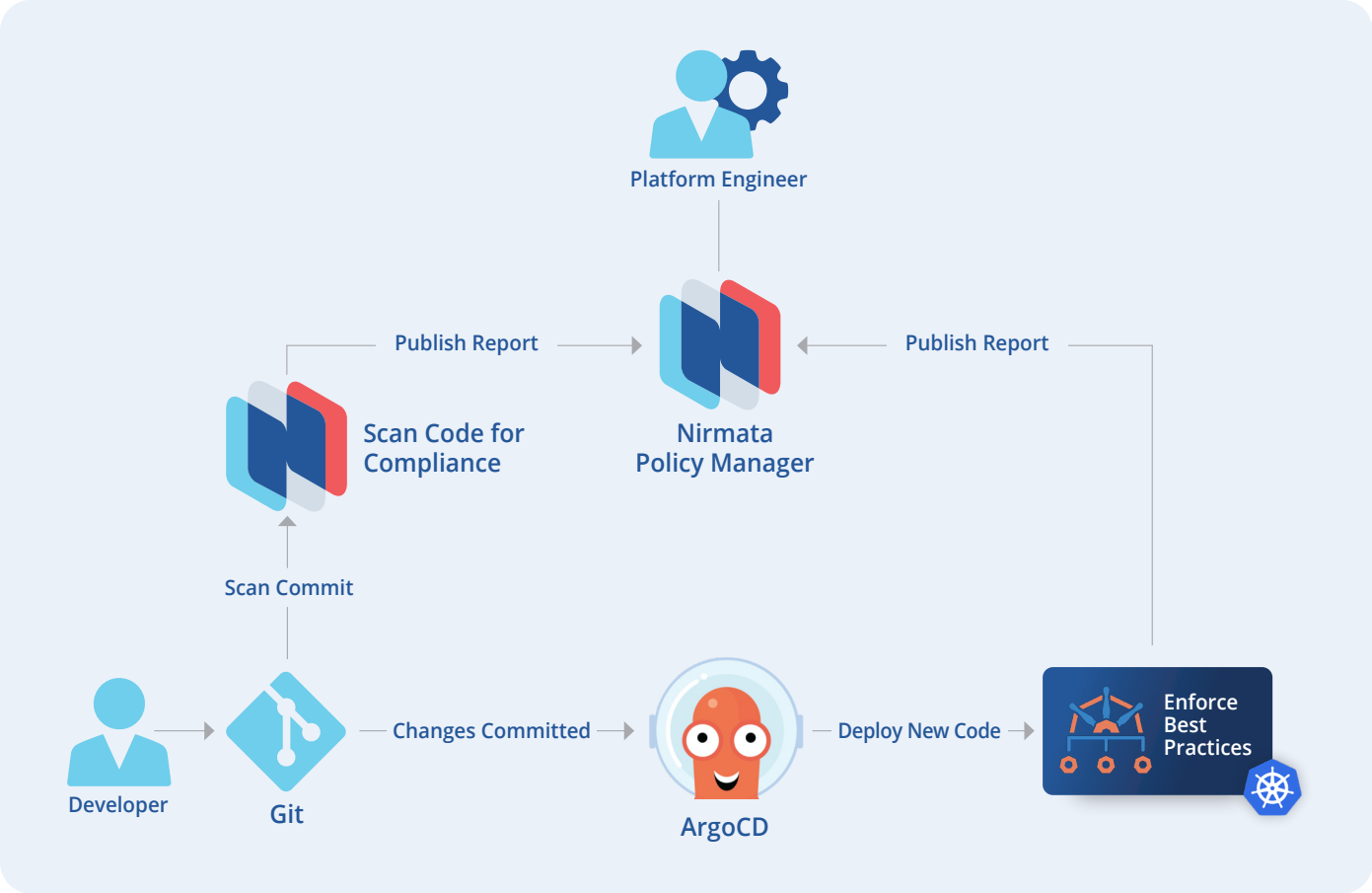
Get Secure, Streamlined, and Developer-Friendly GitOps



GitOps offers a powerful approach to Kubernetes management, but it can introduce security risks, compliance gaps, and operational complexity. Developers need ways to reliably manage cluster and application configurations while ensuring security and preventing costly misconfigurations.

Configuration management is critical to ensuring deployments reliability and security in the context of cluster management. It means treating configurations like akin to code, such as:

- Leveraging version control systems
- Automating deployments
- Implementing policies and compliance checks
- Prioritizing security
- Establishing monitoring and alerting mechanisms
- Providing comprehensive documentation and training to developers

Platform teams and cloud architects require tools for centralized visibility, consistent policy enforcement, flexibility, and streamlined operations, but integrated technologies have only now existed.

SOLUTION

Nirmata, powered by the leading cloud-native policy engine Kyverno, provides a comprehensive solution to secure and streamline GitOps, empowering developers and ensuring robust governance:

- **Policy as Code:** Kyverno enables users like you to define flexible security, compliance, operations, and cost-control policies as Kubernetes resources.
- **Shift-Down Security, Observability, and Developer Empowerment:**
  - **Nirmata CLI (nctl):** Integrates with Git workflows (e.g., GitHub Actions) to scan pull requests (PRs) against established policies, providing early feedback and preventing issues before deployment.
  - **Nirmata Pipeline Scanning:** Use Nirmata's nctl tool to scan Kubernetes, Terraform, Dockerfile, and any structured JSON data manifests in your CI/CD pipelines, detecting potential misconfigurations early in the development lifecycle.
  - **Nirmata Dashboard:** Offers cross-cluster visibility into policies, facilitating troubleshooting, and identifying areas for improvement.
- **In-Cluster Enforcement:** Kyverno validates and mutates resources to safeguard your desired state. You can prevent misconfigurations or detect and report them.
- **Secure and Scalable Argo CD Deployment:**
  - **AWS Best Practices:** Design a secure Argo CD environment using EKS, secrets management, and IAM roles with least-privilege principles.
  - **Agent-Based Architecture:** Leverage agent-based model for simplified deployment, enhanced scalability, and reduced attack surface.
- **Support for Mission-Critical Operations:** Benefit from the commercial support and enterprise features that Nirmata offers.

BENEFITS

- **Enhanced Security:** Reduce risk through proactive policy enforcement, GitOps-integrated security checks, and pipeline scanning.
- **Developer Agility and Streamlined Workflows:** Rapidly deploy intelligent guardrails by implementing curated policies. Guide developers with self-service capabilities, actionable feedback within familiar Git workflows, and early detection of misconfigurations.
- **Operational Efficiency:** Optimize policy management, auditing, and remediation across your Kubernetes clusters. Leverage existing processes and workflows through integration with tools like Git, Slack, Jira, and more.
- **Optimized Resource Utilization:** Enforce resource limits and best practices to prevent uncontrolled costs. Restrict workloads from using expensive resources such as high-throughput storage or GPUs.
- **Centralized Visibility and Control:** Provide cloud architects with centralized policy management, cross-cluster visibility, and operational insights. Immediately detect changes to global policies and enable tamper prevention to ensure that policies are consistently applied.
- **Flexibility and Scalability:** Adapt to growing infrastructure complexity, evolving security standards, and multi-cloud or hybrid environments. Gain insights on the effectiveness of policies through aggregated reporting across clusters to allow focus on the most critical issues.

HOW TO GET STARTED

1. **Install Argo CD:** Deploy the core pillar of your GitOps infrastructure.
2. **Deploy Nirmata:** Integrate Nirmata for cross-cluster policy management, enforcement, and pipeline scanning.
3. **Define Policies:** Collaborate with the security, platform, and development teams to create Kyverno policies that align with your objectives.
4. **Integrate nctl:** Add nctl to CI/CD pipelines for policy checks and integrate nctl for pipeline scanning.
5. **Monitor and Refine:** Use Kyverno reports, Nirmata insights, and pipeline scanning results to improve your policies continuously.

ADDITIONAL READING

- 3 Essential Tips for Using Argo CD and Kyverno
- GitOps and Mutating Policies: The Tale of Two Loops

NEXT STEPS

- **Developers:** Experience how nctl in your CI/CD pipeline improves your deployment process and catches errors early.
- **Architects:** Schedule a demo to see how Nirmata›s policy management and cross-cluster visibility can enhance your GitOps strategy.

Let Nirmata elevate your GitOps practices with policy-driven workflows, pipeline scanning, and seamless developer experiences.