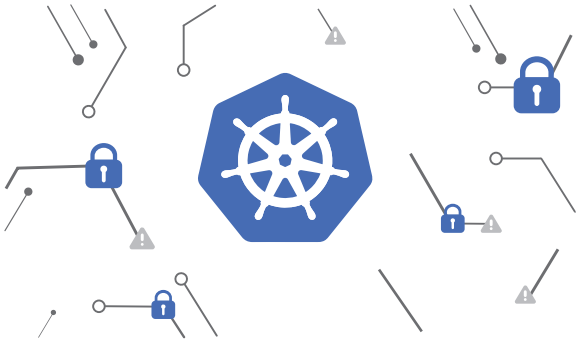
Concourse Labs

Essential code-to-cloud security governance platform, unifies cloud security posture across multi-cloud environments, automates the detection of misconfigurations, provides remediation guidance and enforces security policies at scale.

Kubernetes Challenges

- Kubernetes has emerged as the prime container orchestration tool, but default configurations are often open and insecure.
- Just checking container images for CVEs is not enough to protect your infrastructure from vulnerabilities. For example, administrators must verify that containers do not run as root, secret storage has been encrypted, and pod security context and RBAC controls have been defined.
- Designing, developing, and maintaining workload-specific security and network policies is daunting, and container security expertise is hard to find.
- Microservices and container architectures evolve rapidly. Without automated guardrails it is impossible to ensure continuous security and compliance.



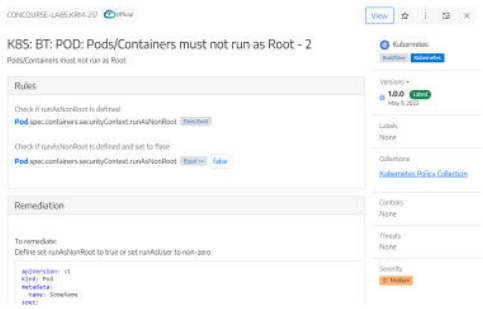
Why Concourse Labs for Kubernetes

Concourse Labs security-as-code provides automated and continuous security checks throughout the development process. Author and apply policies to your Kubernetes environment, whether you're using Kubernetes Resource Model (KRM) files, Helm charts, or Argo rollouts.

- Fast and extensible way to check common misconfiguration mistakes, as well as those specific to your particular architecture and configuration choices
- Auditable security guardrails provide visibility into DevSecOps adoption and catch mistakes before they become exploitable security vulnerabilities
- Automation enables you to scale Kubernetes security across your organization and ensure continuous compliance

Unlock Enhanced Security for Kubernetes with Concourse Labs

- **Automated Security Checks:** Concourse Labs preemptively checks your KRM files, Helm charts, Argo rollouts, and other Kubernetes resources, identifying potential security vulnerabilities before they are deployed. Proactive, preventative controls significantly reduce the chance of deploying insecure infrastructure and applications.



- **Assured Regulatory Compliance:** Whether CIS, CSA, PCI-DSS, GDPR, HITRUST, or FedRAMP, Concourse Labs makes sure your Kubernetes resources adhere to industry standard and best practice security controls and policies.
- **Reduced Human Error:** Human error can lead to critical security breaches. With Concourse Labs, security becomes codified, minimizing the risk of errors that can compromise your cloud infrastructure and applications.

- **Minimized Remediation Time:** Early detection equals early action. Identifying vulnerabilities pre-deployment reduces the time, effort, and cost of remediation.
- **Enhanced Collaboration:** Security and development teams often exist in silos. Break down the walls with transparent policy and clear, actionable remediation guidance for Kubernetes resources.
- **Realized Value:** Automated security and policy for K8s architecture reduces risk of human error and system compromise.
- **Outcome:** Compliance posture reporting demonstrates proof you are operating Kubernetes environments with best practice security controls

concourse LABS

See, fix, and prevent risk for any application, any data, on any cloud, at every point in time

See It.

- Identifies security risks on **any cloud** and in **any infrastructure or workload**
- Finds misconfiguration risk **during development and at runtime**
- Transforms cloud security posture from manual, fragmented and opaque to **automated, unified and transparent**

Fix It.

- Provides **real-time remediation guidance**
- Gives developers real-time, where-they-work, **actionable insight** into security compliance requirements

Prevent It.

- Integration into development workflows **prevents misconfiguration** from reaching deployed environments
- **Continuous, automated monitoring** of runtime environments detects risks and drift from compliant state

While others take a fragmented approach to governing cloud risk, Concourse Labs unifies:

- **Asset Inventory**
- **Infrastructure-as-Code Scanning**
- **Continuous Runtime Monitoring**
- **Remediation Guidance and Tracking**
- **Compliance Posture Management**
- **Policy-as-code Lifecycle Management**

concourse LABS

Automated Security Governance

Across diverse clouds, technologies, stakeholders, workflows