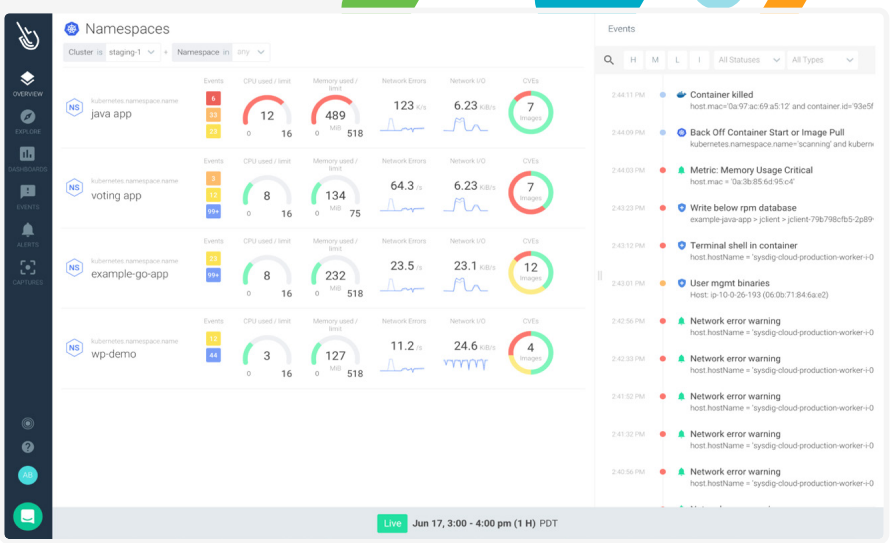
Secure DevOps Platform

sysdig.com/platform

As cloud native becomes the standard for application deployment, IT roles must adapt. Cloud teams are taking ownership for security, as well as application performance and availability. Tools must support a secure DevOps workflow to run Kubernetes and containers in production.

Confidently run cloud-native workloads in production using the Sysdig Secure DevOps Platform. With Sysdig, you can embed security, maximize availability and validate compliance. The Sysdig platform is open by design, with the scale, performance and usability enterprises demand.



Sysdig Benefits

Embed Security

- Detect vulnerabilities and misconfigurations with a single workflow
- Block threats without impacting performance using Kubernetes controls
- Conduct forensics even after the container is gone

Maximize Availability

- Prevent issues by monitoring performance and capacity
- Accelerate troubleshooting with a single source of truth
- Scale Prometheus monitoring across clusters and clouds

Validate Compliance

- Verify configuration meets CIS best practices
- Ensure application compliance with NIST, PCI
- Enable audit by correlating Kubernetes activity

Key Use Cases

Image Scanning
Scan images directly in CI/CD pipeline and identify new vulnerabilities or misconfigurations in production

Configuration Validation
Ensure configuration meets security best practices based on CIS Benchmarks

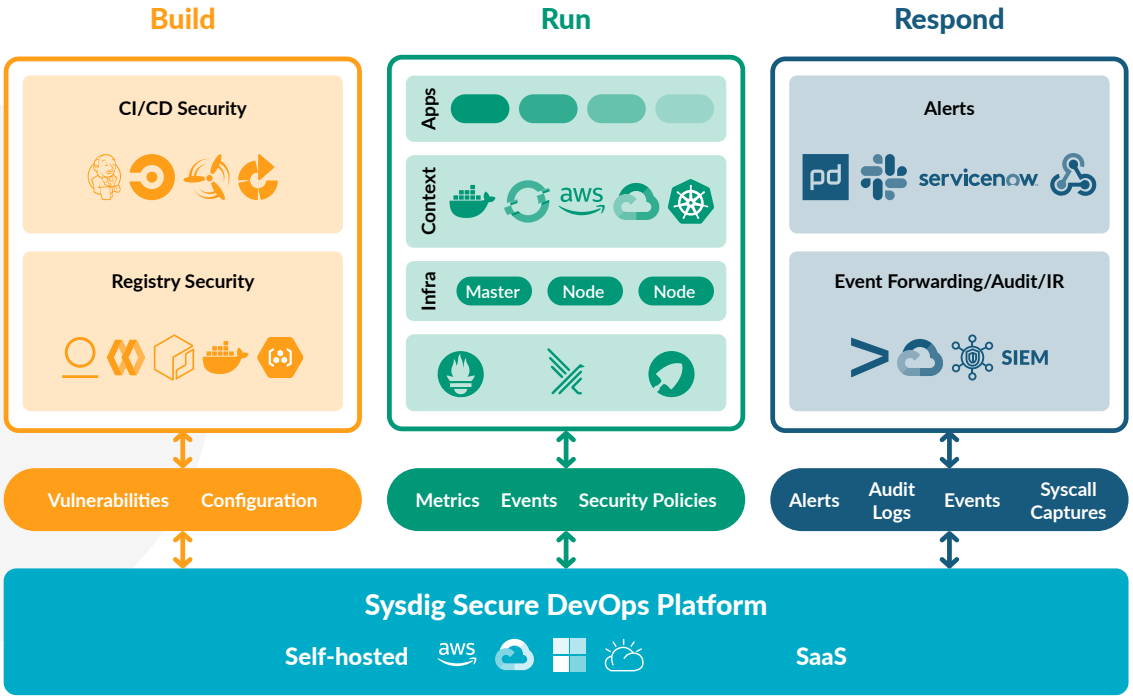
Kubernetes Monitoring
Monitor infrastructure and applications with (Prometheus, JMX, StatsD) metrics using dashboards and topology maps

Runtime Security
Detect anomalous behavior with the Falco engine and prevent threats using Kubernetes native controls such as Pod Security Policies

Continuous Compliance
Ensure compliance across container lifecycle for standards like NIST and PCI

Audit and Incident Response
Reconstruct system activities correlated with Kubernetes application context for forensics and incident response

Unified Workflow Across the Cloud-Native Lifecycle



Build | Run | Respond

Sysdig Secure DevOps Platform

Adds scale, workflow, Kubernetes, and cloud context

Image Scanning
Vulnerability detection

Monitoring
Infrastructure and application metrics

Runtime Security
Detection rules and alerts

Forensics/ Troubleshooting
Deep visibility into container activity

Platform Built on an Open Foundation

Sysdig Secure DevOps Platform enriches open-source data sources (Anchore engine, Prometheus monitoring, Falco rules and sysdig oss) with cloud and Kubernetes application context. With a unified workflow you can run cloud-native workloads confidently at scale.