Secure Kubernetes on Google Cloud Platform with StackRox

StackRox integrates with the Google Cloud services you use to protect your cloud-native workloads throughout the container lifecycle.

The StackRox Kubernetes Security Platform

- Visibility
- Vulnerability Mgmt
- Compliance
- Network Segmentation

- Risk Profiling
- Configuration Management
- Threat Detection
- Incident Response

Google Kubernetes Engine (GKE)
Get Kubernetes-native visibility compliance, risk profiling, and threat detection across all your GKE clusters.

Google Container Registry (GCR)
Secure your images with data from public or private GCR repositories, including vulnerabilities from GCR Container Analysis.

Container-Optimized OS (COS) from Google
Detect attack in your Kubernetes clusters running on COS at runtime and use multi-factor risk profiling to prioritize the deployments that need immediate fixing.

Google Cloud Security Command Center (Cloud SCC)
Enhance your Cloud SCC dashboard with critical risk context and runtime threat detection for your Kubernetes clusters.

“StackRox delivers business-critical threat detection capabilities to Kubernetes users, and this collaboration enables strong runtime security controls for enterprise applications running on Google Cloud.”

— Aparna Sinha, Group Product Manager, Kubernetes and GKE, Google Cloud
Richer Context

The StackRox platform evaluates risk using a deployment-centric view, incorporating a wide variety of factors. CVEs aren’t enough: the same vulnerability poses a higher risk in a publicly exposed production service than in an isolated development container.

Native Enforcement

Deep integration with Kubernetes enables the StackRox platform to tap into the power of open source development, providing a more robust, scalable security. You get universal, portable controls and full alignment between DevOps and Security. StackRox leverages Kubernetes to contain and respond to security issues, and our visualization and simulation capabilities simplify network policy enforcement and secrets management.

Continuous Hardening

The feedback loop at the heart of the StackRox platform applies learnings across the container life cycle to constantly shrink the attack surface. Data from build and deployment enables more accurate detection, and runtime activity monitoring yields.

StackRox helps enterprises secure their containers and Kubernetes environments at scale. The StackRox Kubernetes Security Platform enables security and DevOps teams to enforce their compliance and security policies across the entire container life cycle, from build to deploy to runtime. StackRox integrates with existing DevOps and security tools, enabling teams to quickly operationalize container and Kubernetes security. StackRox customers span cloud-native start-ups Global 2000 enterprises, and government agencies.