uptycs SRC CYBER SOLUTIONS LLP

Solution Brief

Uptycs for Kubernetes and Container Security

Achieve DevSecOps excellence by aligning and simplifying how developers and SecOps work together to secure K8s infrastructure – from laptop to code to cloud.

Go beyond point-in-time visibility

Uptycs unifies Kubernetes security posture management and workload runtime protection into a single security console. You get unified visibility and protection across developer endpoints, GitHub pull requests, software pipelines, and Kubernetes infrastructure residing in both private and public clouds. Gain real-time visibility into your cluster and container fleet and prioritize risks emanating from vulnerabilities, non-compliance, and threats mapped to the MITRE ATT&CK framework.

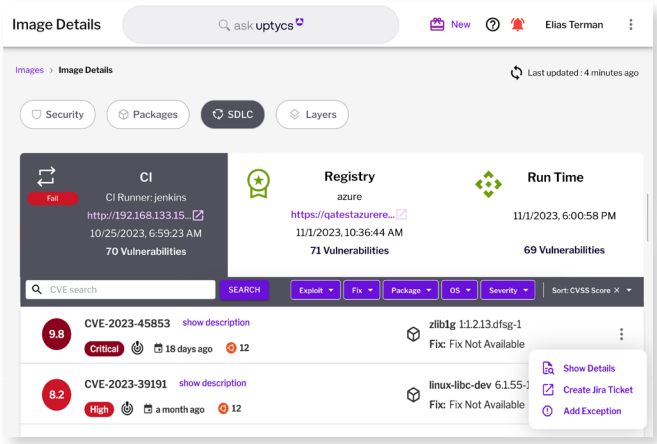
Reduce risk with deeper security measures across the Kubernetes supply chain

Uptycs gives DevSecOps teams end-to-end visibility, image traceability, and security of software supply chain components, including source code repositories, CI systems, container registries, and Kubernetes runtime. Create custom policies and incorporate CIS Software Supply Chain benchmarks to enforce source, build, and deployment integrity across your Kubernetes infrastructure.

With Uptycs, you can take a proactive stance to ensure issues are addressed before they reach production. Automate security early in the software development lifecycle (SDLC) by scanning for vulnerabilities, malware, and secrets across CI/CD pipelines, container registries, and developer laptops. Conduct IaC scans across your code repositories to find insecure Kubernetes configuration files and Helm charts.

Don't just detect. Defend.

Leverage real-time remediation actions and forensics such as YARA rule scanning, file integrity monitoring, and admission controls to block malicious processes and insecure components from deployment. Align on remediation guidelines through policy controls to prevent insecure container images with vulnerabilities, malware, and secrets based on Indicators of Compromise.



Uptycs gives you full image traceability and security across the SDLC from developer build (CI) to runtime

> "Uptycs offers more transparency and flexibility for Kubernetes threat detection than other security vendors. Visibility over our whole cloud environment is absolutely fundamental to our security posture. We can't secure what we can't see."
>
> **Cloud Security Engineer, Top 10 Internet Site**

Discover

Know what you have so you can protect it.

Kubernetes overview graph with asset drill down: identify online and offline clusters, along with their associated nodes, namespaces, pods, and containers.

Real-time risk analysis: quickly surface your highest-risk clusters and containers based on vulnerabilities, threats, and non-compliance. Drill all the way down to processes and file systems.

Consistency across diverse environments: protect and monitor clusters on managed cloud providers like Amazon EKS, Google GKE, Azure AKS, Red Hat OpenShift, VMware Tanzu, and unmanaged Kubernetes. Establish full coverage for self-managed containers such as ECS, Fargate, and containers running in VMs.

Audit

Identify what's wrong so you can fix it.

KPI-based vulnerability management: monitor vulnerabilities and prioritize remediation efforts based on high impact vulnerabilities with known exploitations or available fixes across CI, registries, and runtime containers

Compliance management: monitor compliance posture for CIS Benchmarks, PCI, SOC 2, and NSA Hardening with real-time evidence and remediation.

Shift-left image scanning: continuously scan images throughout the SDLC with automated vulnerability, malware, and secrets scanning. Start with CI tools like Jenkins and move to container registries such as Artifactory.

Secure

Respond to suspicious behavior so you can secure it.

Real-time threat detections: Map data plane threat information to the MITRE ATT&CK framework. See how threats are correlated with K8s control plane misconfigurations for rapid threat mitigation.

Container runtime protection: optimize your threat hunting and investigative capabilities using anomaly detection and runtime tools, including YARA file/ memory scanning, container process blocking and remediation, and the ability to conduct real-time and historical queries across your Kubernetes environments.

RBAC access monitoring: visualize and prioritize key access control risks. Take a proactive approach to minimize lateral movement attack vectors and stop unauthorized exposure of secrets in shared cluster environments.

Policy enforcements (image admission controller and open policy agent gatekeeper): apply runtime protection to block insecure pod deployments. Implement out-of-the-box or your own custom OPA Gatekeeper policies to block insecure Kubernetes infrastructure from being deployed. Leverage image policies based on critical vulnerabilities to block risky images from deployment.

Broad ecosystem support

Kubernetes Cluster Types	Amazon EKS, Google GKE, Azure AKS, Red Hat OpenShift, VMware Tanzu, Unmanaged (On-Prem or Cloud)
Self Managed Container Types	Amazon ECS, Fargate, Google GCE, Azure Container Service Any container running on VMs or bare metal
Container Runtime	Docker, CRI-O, Containerd
Image Registries	JFrog Artifactory, Amazon ECR, Google GCR, Azure ACR, Private Docker Registry (Cloud + On-Prem)
CI Pipeline	Jenkins, GitHub Actions, GitLab, AWS Codebuild, Travis CI
IaC Scanning	Terraform, CloudFormation, Helm, Kubernetes YAML, Dockerfile
Compliance Standards	CIS (Kubernetes, EKS, GKE, AKS + Docker), SOC2, PCI, NSA Hardening
3rd Party SaaS	IdPs: Okta, Azure AD Code Repositories: GitHub
Developer Enpoints	macOS, Linux, Windows, Cloudflare ZTNA

About SRC

At SRC Cyber Solutions LLP , we provide Next Generation , Highly Automated , User - Friendlyand scalable solution . Our robust solutions include Comprehensive Email Security , Automated Patching and Endpoint Management , Asset Risk Visibility and Management with Policy Enforcement (ARM), Third - Party Data Flow Security solutions, Agentless Micro Segmentation, Endpoint, Management, and, Compliance Platform and an Online Gamified Simulation Platform for Cyber Security Training attacks . Additionally , we provide a Cloud - Native Application Protection Platform (CNAPP) solution to ensure comprehensive security across cloud - native applications.

www.srccybersolutions.com | +91 120 232 0960 /1 | sales@srccybersolutions.com

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

uptycs

022124