www.uptycs.com

# UPTYCS KUBERNETES AND CONTAINER SECURITY CAPABILITIES

Uptycs

## Uptycs Kubernetes and Containers Capabilities

When Kubernetes and container deployments scale up, it becomes difficult to inventory and monitor your fleet. To solve your problems around Kubernetes and container workflows, the Uptycs unified CNAPP and XDR solution offers a single place to get clear visibility across your container assets. You can also see your compliance posture, identify and prioritize vulnerabilities, and detect threats in real-time. You can unify security management from build stage through to runtime deployments.

Uptycs offers Kubernetes security posture management (KSPM) and cloud workload protection (CWPP) to cover a broad range of security use-cases, and the flexibility to rapidly add more given the breadth and depth of telemetry:

- Visibility
- Vulnerability management
- Registry scanning
- Policy audit / enforcement
- Compliance
- Threat detection
- Remediation and forensics

| Use Cases | Description |
|---|---|
| **Visibility** | • Comprehensive telemetry for control plane & nodes<br>  • **Control plane:** 50+ tables covering all K8s objects like Pods, Deployments, ConfigMaps, Ingress, RBAC<br>  • **Node:** Granular container & host telemetry covering processes, files, DNS lookups, sockets and more<br>• Multi-cluster visibility into compliance, threats and vulnerabilities through a single pane of glass. Granular view into namespaces, pods, workloads for any infrastructure questions<br>• Retroactive investigation capabilities with flexible data retention options<br>• Support for AWS Fargate and node telemetry on OpenShift |
| **Vulnerability Management** | • Support for Build-time & Run-time scans with Deploy-time enforcement<br>  • **Build-time:** Integration with CI pipeline with ability to fail builds<br>  • **Deploy time:** Enforce customizable policies using built-in K8s admission controller<br>  • **Run-time:** Periodic re-scans of containers with new vulnerability feeds<br>• Support for vulnerability exceptions<br>• Scan for 60k+ Linux CVEs<br>• Broad Linux support: Alpine, Amazon Linux, CentOS, RHEL, Ubuntu & others |
| **Registry Scanning** | • Scan newly added images and schedule scans of existing images for vulnerabilities<br>• Scan for secrets and sensitive data<br>• Automated registry scanning based on any new CVE<br>• Apply exclusion list for image scanning<br>• Fail images based on vulnerability severity during deployment through Gatekeeper OPA<br>• Fail/Recall images containing secrets and sensitive data during build and deploy times |

| Use Cases | Description |
|---|---|
| **Policy Audit / Enforcement** | • Embedded Gatekeeper (OPA) support for both Audit and Enforcement modes<br>• Gatekeeper events logs available in telemetry<br>• Support for all Gatekeeper constraint templates |
| **Compliance** | • CIS benchmarks for K8s, AKS, EKS, GKE<br>• SOC2 & PCI checks on nodes [Q1]<br>• Ability to customize checks for any compliance standard<br>• Auditor-ready reports with evidence to support findings<br>• NSA Kubernetes hardening checks - Avoid common misconfigurations and implement recommended hardening measures (e.g. network separation, pod security policy) |
| **Threat Detection** | • Container runtime and kubernetes specific threats<br>• 3 types of threat detections:<br>  • **Behavior:** 150+ rules out of the box mapped to MITRE ATT&CK<br>  • **Contextual:** Yara scanning of container processes with 200+ rules<br>  • **IOCs:** Monitor known bad domains and IPs<br>• Custom rule definitions for new behavior techniques<br>• Monitor privileged containers, including root usage, host access, enhanced Linux capabilities, SELinux settings etc) |
| **Remediation and Forensics** | • Remediation capabilities e.g. kill container, pausing container, quarantine node<br>• Process and file carving |

| Eco-systems Supported | |
|---|---|
| **Image Registries** | JFrog Artifactory, AWS ECR, Google Container Registry, Azure Container Registry, Docker hub |
| **Container Runtime** | CRI-O, ContainerD, Docker |
| **Orchestrations** | Google GKE, AWS EKS, Azure AKS, Kubernetes, OpenShift, VMware Tanzu, Google Anthos, Self-managed containers |
| **CI Plugins** | Jenkins, AWS Codebuild, Gitlab, Github Actions |
| **CD Plugins** | Helm Charts |

# About Uptycs

Your developer's laptop is just a hop away from cloud infrastructure. Attackers don't think in silos, so why would you have siloed solutions protecting public cloud, private cloud, containers, laptops, and servers?

Uptycs reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single platform, UI, and data model. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive enterprise-wide security posture.

Looking for acronym coverage? We have that, too, including CNAPP, CWPP, CSPM, KSPM, CIEM, CDR, and XDR. Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

**Shift your cybersecurity up with Uptycs.**

**Learn how to at:**
**https://www.uptycs.com**