



KUBERNETES SECURITY POSTURE MANAGEMENT (KSPM) & CONTAINER SECURITY WITH ORCA

THE CHALLENGE:

Ephemeral Workloads, Hidden Identity Risk, and Fragmented Tools

According to Orca's State of Cloud Security Report, Kubernetes now runs in 70% of organizations' cloud environments, and every cluster adds layers that traditional cloud security tools were never built to see, such as namespaces, workloads, RBAC bindings, and container images that spin up and disappear in minutes. Misconfigurations are common, and 82% of organizations have a publicly accessible Kubernetes API server.

The bigger problem is that Kubernetes risk doesn't stay inside the cluster. 93% of organizations have at least one privileged Kubernetes service account, and through mechanisms like IRSA and Workload Identity, those accounts are often tied directly to cloud IAM roles. A vulnerable container running with an over-permissioned service account isn't just a cluster finding. It's a path to the cloud data behind it. Container-only tools stop at the cluster boundary and cloud-only tools never look inside it, so that connection goes unseen.

What teams need instead is one view that connects cluster posture, image vulnerabilities, runtime activity, and cloud identity, and that helps them fix issues at the source before they reach production.

THE SOLUTION:

Visibility, Context, and Prevention in One Platform

Orca's KSPM and Container Security runs on the same agentless SideScanning™ technology and Unified Data Model that power the Orca Platform. Every cluster, workload, and image is automatically connected to the identities, network exposure, and cloud resources around it, so findings arrive with an attack path attached instead of as isolated alerts.

✓ Complete Visibility

Managed and self-managed clusters connect automatically or through an outbound-only connector, with coverage of containers and images before a cluster is onboarded and an optional sensor for real-time runtime detection.

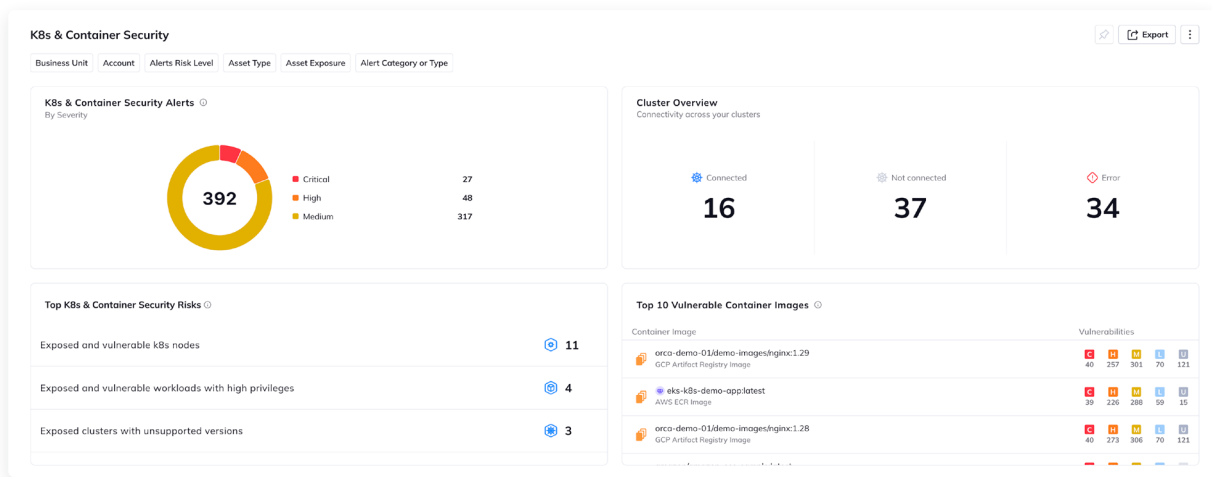
✓ Context That Powers Decisions

Image vulnerabilities, misconfigurations, and RBAC permissions are correlated with network exposure and cloud IAM to surface Kubernetes attack paths, like a vulnerable container whose service account maps to an over-permissioned cloud role, so teams fix what's actually exploitable first.

✓ Security That Fits the Way You Work

Policies are enforced in CI and at deploy time, findings trace back to the Helm chart or Dockerfile and the team that owns it, and remediation routes directly into the integrations with the ticketing, SIEM, and CI/CD tools teams already use.





KSPM & Container Security Capabilities

- **Complete Cluster Coverage, Agentlessly:** Connects to managed Kubernetes on every major cloud, including EKS, AKS, and GKE, plus self-managed clusters and OpenShift, public or private, in cloud or on-prem. Agentless SideScanning shows what's running on nodes even before a cluster is onboarded.
- **Kubernetes Posture Assessment:** Continuously checks workloads, RBAC, services, ingresses, and network policies for misconfigurations, flagging privileged or root containers, privilege escalation, and clusters nearing end-of-life support.
- **Admission Controller:** Stops risky workloads before they reach production by enforcing centrally managed policies at deploy time. Built-in controls block privileged containers, untrusted registries, and mutable image tags, and audit mode lets teams see a policy's impact before switching to block.
- **Image Trust:** Connects what was scanned in CI to what's allowed to deploy. Every container image is checked against its scan verdict at deployment, and images that failed, have an outdated scan, or optionally were never scanned are blocked. Mutable tags are resolved to immutable digests first, so the image that runs is the exact image that passed.
- **Compliance Mapping & Reporting:** Maps findings to 200+ pre-built and customizable compliance frameworks and benchmarks, including the CIS Kubernetes Benchmark, CIS Benchmarks for EKS, AKS, and GKE, Kubernetes STIG, OWASP Kubernetes Top 10, PCI DSS, CIS Docker Benchmark, and NIST 800-190, with one-click export for audit-ready compliance reports.



By offering a seamless scan with the agentless functionality, the solution is transparent. We can scan our managed resources like containers in Kubernetes, and Orca gives us suggested improvements for roles and identity management."

SÉBASTIEN GAUCHER
IT Operations Manager





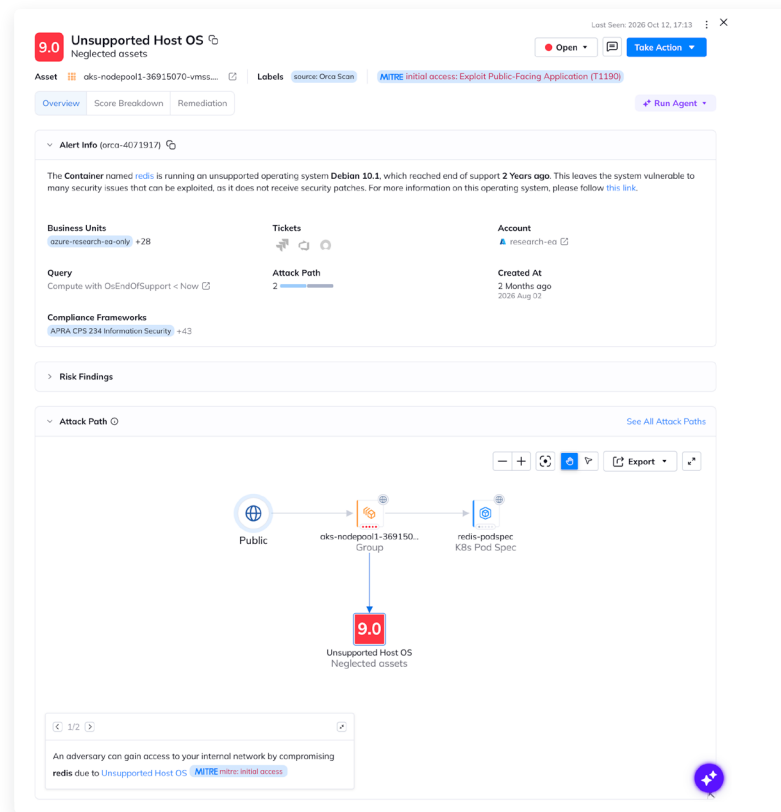
- **Container Image Vulnerability Scanning:** Enriches every CVE with EPSS, CISA KEV, exploit, and patch data, and prioritizes the images that are actually running. Containers built on unsupported base OS distributions are flagged automatically. SBOMs can be exported in CycloneDX or SPDX.
- **Registry and Pipeline Scanning:** Scans images in ECR, ACR, GCR/Artifact Registry, Docker Hub, and JFrog Artifactory. The Orca CLI catches issues in CI before images are pushed, and IaC scanning checks Kubernetes manifests and Helm charts before they deploy.
- **Kubernetes Attack Paths:** Traces how an attacker moves from a compromised container through Kubernetes RBAC to admin-level access, then through IRSA and Workload Identity to the cloud IAM roles behind them, mapping risk past the cluster boundary instead of stopping at it.



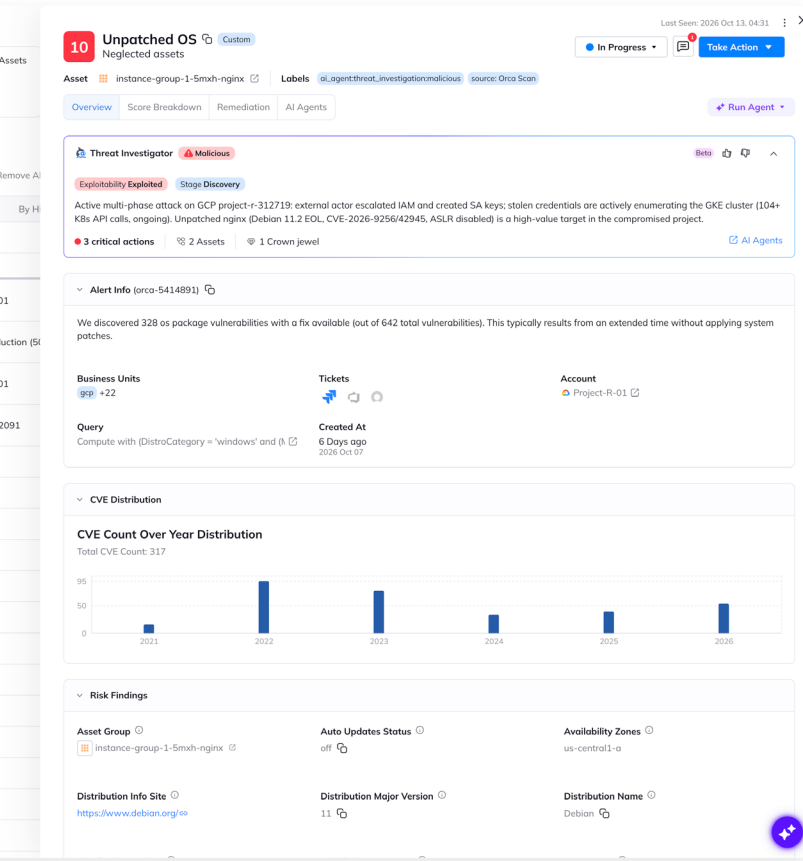
Anybody in an engineering organization or who is deploying artifacts into a cloud environment will benefit from Orca Security. It gives us insight into everything that's being spun up and anything that may be misconfigured."

AARON BROWN

Senior Cloud Security Engineer



- **Risk-Ranked Kubernetes Dashboard:** Surfaces the top clusters at risk, most vulnerable images, publicly exposed services, and over-privileged vulnerable workloads, with drill-down to the underlying assets and alerts.
- **Orca Sensor for Runtime Threat Detection:** An optional, lightweight eBPF sensor catches attacks in progress inside running workloads, such as container escapes, service account token theft, and crypto mining, so teams can respond before an attacker moves deeper into the cluster or cloud. Detections are mapped to MITRE ATT&CK to speed up investigation, and coverage extends to serverless containers on Fargate and GKE Autopilot.
- **Integrations:** Expansive integration capabilities include Jira, ServiceNow, Splunk, Slack, and GitHub, and span key categories such as Ticketing, Notifications, SIEM & SOAR, Identity & Access, GRC & Compliance, Storage, CI/CD & Endpoint, and AI & MCP, plus webhooks and a documented API.



- **Automations and AI Agents:** Orca Automations trigger ticketing, notifications, and remediation actions on defined rules, while Orca AI Agents can investigate alerts and generate ready-to-run remediation code, then open a pull request or ticket for supported scenarios. A Kubernetes attack path's full detail, including its timeline and story, can also be pushed into a new Jira ticket in a single action.
- **Cloud-to-Dev Code Origin:** Traces risky workloads back to the Helm chart or Dockerfile, repo, and code owner that defined them, so fixes reach the right team.
- **Guided Remediation Recommendations:** Every finding comes with step-by-step remediation guidance mapped to its specific misconfiguration, vulnerability, and context, so responders know exactly what to fix and how instead of starting from a blank runbook.
- **Multi-Cluster Governance:** Groups clusters into Business Units and assigns admission and sensor policies per cluster to match how teams are organized.

About Orca

Orca Security delivers security for the companies that build. As cloud, applications, AI and app generation expand the attack surface, Orca transforms security risk into the context teams need to act. The Orca Platform provides complete visibility across cloud, AI, and application environments, correlates risk across every layer, and prioritizes the exposures that matter most so organizations can remediate faster and innovate with confidence.

Trusted by hundreds of organizations, including SAP, Autodesk, Gannett, and Digital Turbine, Orca is backed by leading investors including Temasek, CapitalG, ICONIQ Capital, and Redpoint Ventures.

Learn more at <https://orca.security>.

 **Ready to try it out?**
Sign up for a demo. Visit orca.security/demo

