Orca SECURITY | Chainguard

PROTECT CLOUD NATIVE APPS FROM BUILD THROUGH RUNTIME

The Challenges: Too many CVEs from traditional open source with no clear priority of risk to remediate

Open-source software has risen dramatically in popularity, driving a completely new approach to building, and therefore securing, applications. While the use of open-source software has increased speed-to-market for innovation, it's also made vulnerability management and patching more complex for three specific reasons:

1. **No Fix Available:** Sometimes when a new CVE is discovered in open-source software, there isn't a new version of the software available with the vulnerability fixed. Vulnerability management teams must figure out an alternative way to mitigate risk.
2. **Vulnerable Base Images:** When using a traditional open-source base image with vulnerabilities, these CVEs get multiplied across millions of containers, creating an overwhelming number of vulnerabilities for the team to address.
3. **Hidden Dependencies:** Even when a child software package has a fixed version, parent software packages may still use the old vulnerable version, delaying patch efforts. Dependencies create blind spots.

The Solution: Orca + Chainguard

Chainguard: Build with a Better Base

Chainguard is the safe alternative to traditional open-source software, with a demonstrated 97.6% reduction in CVEs compared to open source equivalents. Chainguard delivers purpose-built distroless container base and app images with zero CVEs, as well as minimal, zero-CVE virtual machine images built entirely from source, and malware-resistant language libraries to keep developers focused on shipping instead of curating and maintaining packages.

Chainguard Containers is a curated catalog of 1,700+ minimal, zero-CVE container images that have a reduced attack surface and come with transparent provenance. Chainguard container images only contain the essential runtime components—no shell or package manager. This significantly reduces the attack surface and makes containers inherently more secure, while also decreasing image sizes and improving performance. These "standard" container images are paired with -dev variants (that are production-ready as well), with the shells and package managers developers often rely on when building their software, allowing teams to leverage multi-stage build processes on the same trusted foundation.

The Challenge:

Overwhelming vulnerabilities with no clear risk prioritization

The Solution:

Build with a better base from Chainguard, focus on high impact remediation with Orca, and simplify continuous compliance with this joint solution.

Chainguard + Orca Benefits:

- ✓ Shrink the attack surface
- ✓ Reduce CVEs and false positives
- ✓ Increase line of sight into the software supply chain
- ✓ Prioritize risks clearly with full context
- ✓ Simplify compliance

Orca: Focus on High Impact Risks with Clear Prioritization

To empower security teams to identify, prioritize, and remediate cloud risks, Orca offers an agentless-first approach to visibility into every layer of your cloud estate—including cloud configurations, host OSes, container images, Kubernetes clusters, open-source components, and more. Orca supports full visibility into images based on Chainguard OS, including Chainguard Containers, enhancing line of sight into the software supply chain. The Orca Platform scans these images and their installed packages for vulnerabilities, validating them against Chainguard Security Advisories and reducing false positives.

Visibility into Chainguard Containers enriches the context the Orca Platform delivers through attack path analysis across other data sources like threat intelligence feeds, code repositories, identity and access management policies, and more. The Orca Platform provides an opinionated view of risk through its dynamic risk scoring of alerts and narrows the focus for remediation through Agentless Reachability Analysis. By showing which CVEs are actually reachable by attackers in production and dynamically assigning numerical scores to alerts, the Orca Platform enables security and DevOps teams to pinpoint which issues are the most critical and focus on higher impact remediation efforts.

Simplify Continuous Compliance with Orca and Chainguard

Chainguard Containers inherently solve compliance for critical frameworks like FedRAMP, PCI-DSS, and SOC 2 with out-of-the-box capabilities. The hardened, continuously updated images come with kernel-independent FIPS validation and OS-level STIGs by default, as well as full build-time SBOMs.

The Orca Platform complements the use of Chainguard Containers with a unified view of cloud compliance. Orca offers over 185 out-of-the-box customizable compliance frameworks to monitor, including PCI-DSS, NIST CSF, ISO 27001, SOC 2, and more. Compliance gaps are connected directly with alerts, making it easy to align remediation with existing alert workflows.

About Chainguard

Chainguard is the secure foundation for software development and deployment. By providing trusted open source software with Chainguard Containers, VMs, and Libraries, built from source and updated continuously, Chainguard helps organizations eliminate threats in their software supply chains. Its customers include Fortune 500 enterprises and global industry leaders, including Anduril, Canva, Fortinet, Hewlett Packard Enterprise, Snap Inc., and Snowflake.

About Orca

Orca offers a unified and comprehensive cloud security platform that identifies, prioritizes, and remediates security risks and compliance issues across AWS, Azure, Google Cloud, Oracle Cloud, Alibaba Cloud, and Kubernetes. The Orca Cloud Security Platform leverages Orca's patented SideScanning™ technology to provide complete coverage and comprehensive risk detection.

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