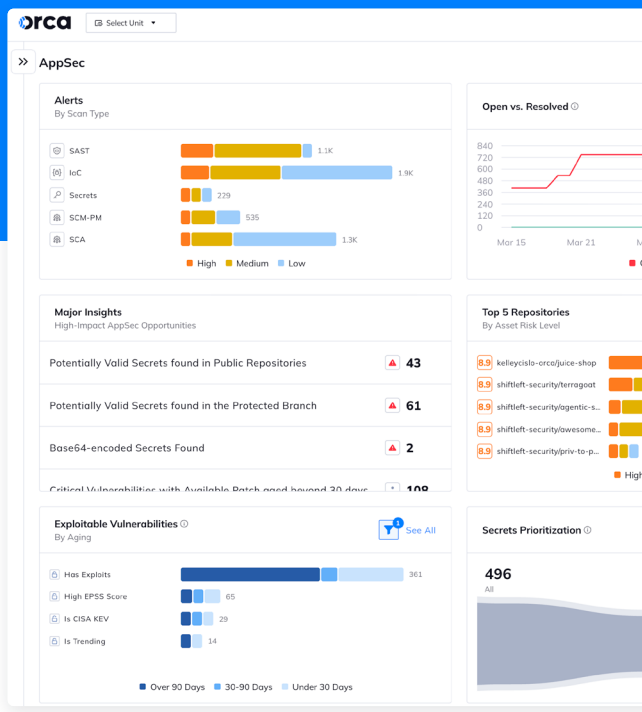
CODE SECURITY WITH ORCA



THE CHALLENGE:

Code Ships Faster Than Security Can Keep Up

90% of developers now use at least one AI coding tool, and code moves from commit to production continuously. Most teams secure it with upwards of seven disconnected point tools, each with its own dashboard and severity scale, leaving DevOps and SecOps working from different versions of the same risk. Meanwhile, the software supply chain has become a routine production risk, with open-source and agent-selected packages entering codebases faster than teams can vet them and 11% of organizations already running known malicious packages in production.

15 MINUTES

from connecting your SCM to scanning every repository, with IDE extensions ready in 5.

CATCH THE RISK, TRACE THE SOURCE

Connect every production risk back to the Dockerfile, Terraform, or Helm chart that created it.

TRUST YOUR CODE

Security confidence in every line, whether a developer, copilot, coding agent, or app generator wrote it.

Many teams are stuck in a cycle of visibility without action. 78% of organizations run applications with critical vulnerabilities, and 77% leave high or critical container vulnerabilities unpatched after 90 days (Orca Security, 2026 State of Application Security Report). CVSS scores the same vulnerability a 9.8 whether it's exposed in production or sits in code that never ships, so teams can't tell which findings put the business at risk. Also, stacking point tools hasn't made risk go away, with 30% of organizations retain recoverable secrets in Git history, 26% don't enforce code review before merging, and logic flaws like broken access controls sit beyond what rule-based scanning is built to find.

THE SOLUTION:

Secure Code From Prompt to Cloud at the Speed It's Built

Orca Application Security scans every pull request and every merge, so security keeps up with code no matter how fast it's written or who writes it. SAST, SCA, secrets detection, IaC scanning, SCM posture, malicious-package detection, and container scanning run in one platform and one risk model, alongside the cloud, AI, and runtime coverage Orca already provides. Empowering teams to fix exploitable risk at the source, before it reaches production.

COPYRIGHT 2026 ORCA SECURITY. ALL RIGHTS RESERVED

- **Complete Visibility:** Orca scans every connected repository, whether the code came from a developer, a copilot, a coding agent, or an app generator like Lovable. Vulnerable and malicious packages, secrets buried in Git history, and risky SCM settings like missing code review all surface in one view. The AI Code Security Auditor extends detection into application logic, reasoning across files to find flaws rule-based scanning isn't built to catch, like broken access controls and tenant isolation failures.
- **Context That Powers Decisions:** Visibility is only as valuable as the priorities it produces. With code and cloud in one risk model, Cloud-to-Dev pinpoints the IaC alerts behind deployed assets that are public-facing, on an attack path, or holding sensitive data. DevOps and SecOps operate from that same view of exposure, replacing the back-and-forth between teams with one shared workflow. Code Reachability confirms which vulnerable dependencies actually run, and the AppSec Triage Agent de-prioritizes false positives in first-party code, leaving a short, ranked list of real risk.
- **Security That Fits the Way You Work:** Fixes arrive where developers already work. AI Code Fix turns confirmed SAST findings into one-click pull requests, and bidirectional Jira sync keeps tickets and Orca alerts aligned, reopening both if a fix doesn't hold. Native MCP support and the Orca Skills hub bring Orca's context into coding agents like Claude Code, Cursor, and Codex. Teams set strict or permissive enforcement for each policy, so critical findings get fixed before they age in a backlog, without slowing development.

Cloud, Code, & AI Security - One CNAPP

- SAST
- SCA
- Secrets Detection
- IaC Security
- Malicious Packages
- Container Images
- SCM Posture
- CI/CD Security
- SBOM & License Compliance
- CSPM
- Compliance
- AI Security

> *Orca moved us from ad hoc scanning to a centralized AppSec approach with real visibility. With Orca, we know exactly where to focus and can stop insecure code from reaching production, even across different tech stacks and siloed products."*

JAKE BARNUM

Radicle Health

How Orca Secures Code

SideScanning™

Alongside native integrations for GitHub, GitLab, Azure DevOps, and Bitbucket, Orca's patented agentless SideScanning™ technology connects code to the cloud it runs in. It powers Cloud-to-Dev, tracing running containers, cloud assets, and Kubernetes resources back to the Dockerfiles, Terraform, and Helm charts that created them, and Agentless Reachability Analysis, which shows which vulnerable functions your code actually invokes before it ships.

Orca Sensor

An optional, lightweight eBPF sensor for teams that need runtime depth. Dynamic Reachability Analysis confirms which vulnerable packages are actually loaded and executed in production, so teams fix what's running first.

Unified Data Model

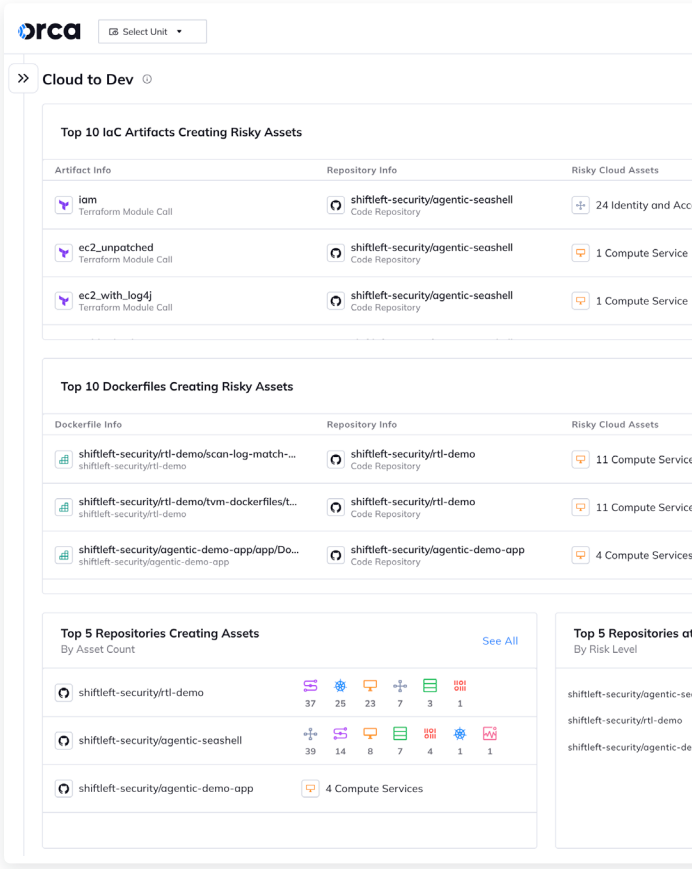
Code, cloud, identity, workload, data, and AI context all live in one graph instead of siloed tools, so every code finding carries the repository and code owner behind it and the cloud exposure in front of it. Teams fix the root cause once instead of patching the same issue in production again.

Dynamic Risk Scoring

Every finding is scored with the full reasoning shown alongside it, and can be prioritized by deployment status, internet exposure, and exploit signals like CISA KEV and EPSS instead of a static CVSS label. Confirmed code reachability raises the score automatically.

Orca AI

A full suite of AI agents built for security and development teams. The AI Code Security Auditor ranks each logic flaw it finds by runtime exposure, sensitive data, and cloud permissions, and pairs it with a data-flow narrative and a fix PR. The AppSec Triage Agent explains each true or false positive verdict with a confidence level. AI Code Fix opens a one-click pull request for confirmed SAST findings, and AI-powered remediation drafts IaC fixes for cloud misconfigurations traced back to code. Native MCP support connects Orca's context into the tools and coding agents your team already uses.



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

COPYRIGHT 2026 ORCA SECURITY. ALL RIGHTS RESERVED