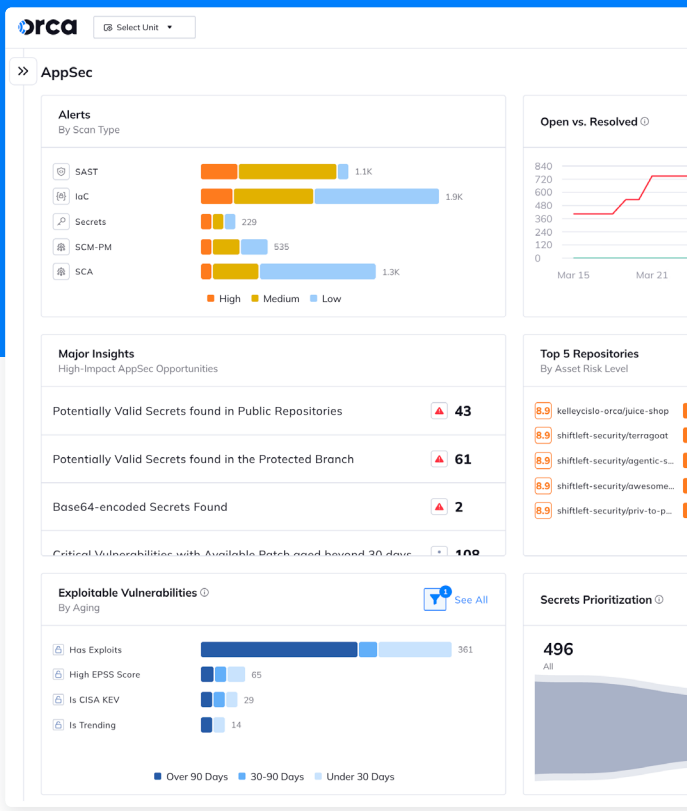
SOLUTION BRIEF

APPSEC WITH ORCA SECURITY



THE CHALLENGE:

Risk is Growing Faster Than It's Being Remediated

Application security programs are under pressure from every direction. Vulnerabilities are consistently making it into production and lingering for months, with 77% of organizations retaining critical vulnerabilities for over 90 days. Expanding software supply chains continue to introduce new and untracked risk, while rapid AI adoption is adding even more complexity to already stretched security teams.

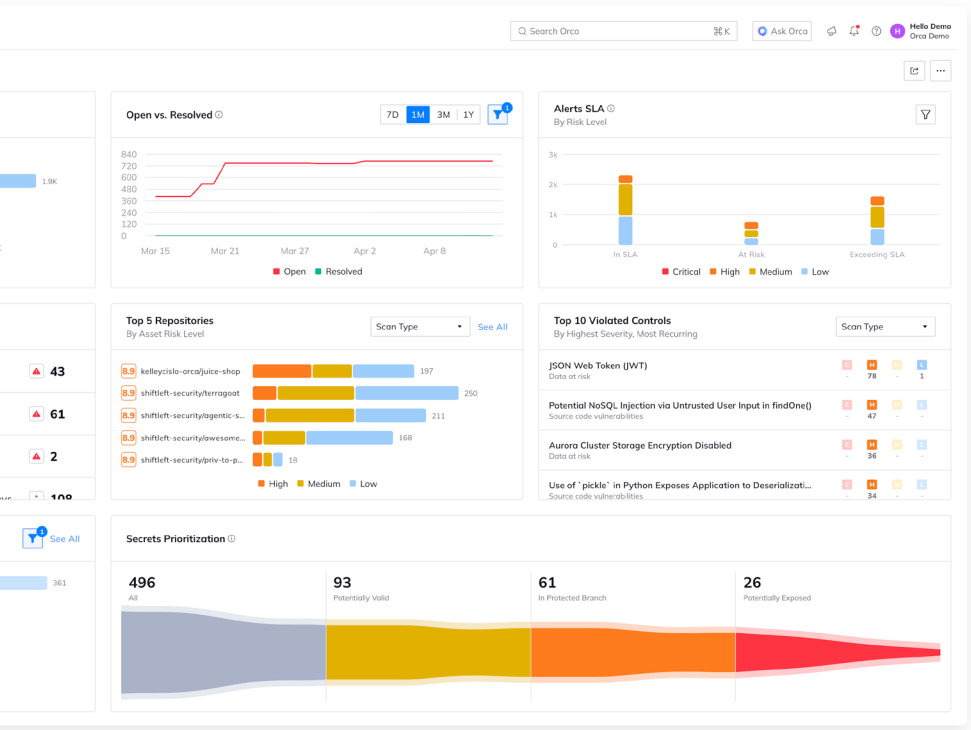
Security teams are overwhelmed with findings but lack the context to understand what is truly exploitable, what poses real business risk, and how to prioritize remediation without slowing development. Many organizations are stuck in a cycle of visibility without action.

THE SOLUTION:

Application Security Across the Lifecycle

Orca unifies application security from cloud to dev, helping teams identify, prioritize, and remediate the risks that matter. By combining code analysis, cloud visibility, runtime context, and AI-driven automation throughout the entire SDLC, Orca transforms AppSec into a streamlined, risk-based workflow.

- ✓ **Identify:** Orca delivers end-to-end visibility across code, dependencies, pipelines, and cloud environments in a single platform. Through deep integrations into SDLC and CI/CD workflows, teams can continuously identify vulnerabilities, exposed secrets, and misconfigurations as they are introduced, while connecting them to the applications and assets they impact.
- ✓ **Prioritize:** Orca delivers dynamic, context-rich prioritization based on real-world risk. By combining code reachability, runtime context, identity exposure, and sensitive data access, Orca determines true exploitability, while attack path analysis maps how risks can be chained across code, cloud, and identities, enabling teams to focus on the issues that pose the greatest business impact.
- ✓ **Remediate:** Orca accelerates remediation by turning insights into action with AI-driven triage, AI-remediation, and automated workflows. Security and development teams can quickly validate findings and fix cloud risk at the source with clear guidance and automated pull requests integrated into existing workflows.



Code

1st Party Code Security

First-party code is analyzed using SAST and IaC scanning to identify insecure code patterns, misconfigurations, and exposed secrets early in development. AI-driven code fix and AppSec Triage Agent validate findings and provide clear remediation guidance within developer workflows.

3rd Party Code Security

Software composition analysis identifies and surfaces the most exploitable vulnerable or risky dependencies, including AI packages, open source license risks, and policy violations using detailed dynamic risk scoring. This enables teams to manage third-party risk and enforce compliance across applications.

Developer Workflows

Integrations into IDEs, pre-commit hooks, and Command Line Interface (CLI) enable issues to be identified early in development. This allows teams to detect and fix insecure code, secrets exposure, and misconfigurations before they leave the IDE.

Build & Deploy

Container Image Scanning

Container images and associated dependencies are scanned using SCA to identify vulnerabilities in the image app and base image OS before deployment, enabling teams to catch inherited and third party risk early so only secure artifacts move through the pipeline.

Security Policy Enforcement

Security policies are enforced through pre-commit hooks, PR checks, and CI security gates to prevent insecure artifacts progressing through the pipeline. Customized policies enable strict or permissive enforcement as needed for consistent security standards without slowing development.

CI/CD Pipeline Security

CI/CD pipelines are analyzed as part of pipeline security and SCM posture management, including GitHub Actions security and flexible CI integrations to ensure the development pipeline itself is secured from risks such as template injection, credential leakage, and more.

> *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

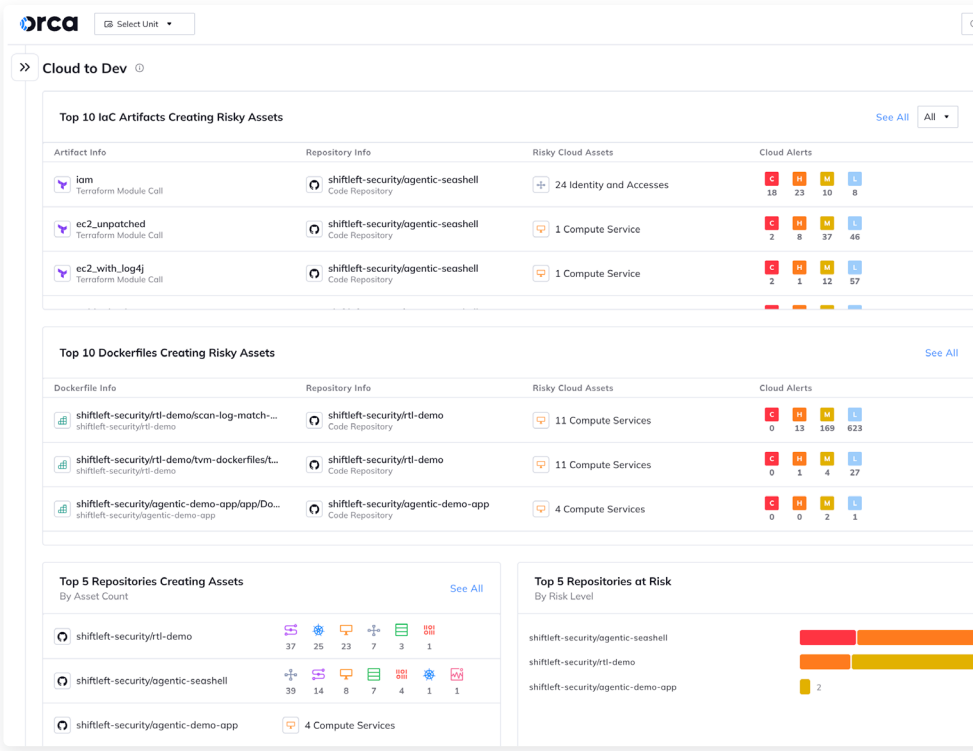
Runtime: Prioritize Exploitable Risk

Cloud to Dev

Cloud assets are mapped back to their originating code, connecting containers to Dockerfiles, cloud assets to Terraform, and Kubernetes resources to Helm charts to provide full ownership and context.

Contextual Risk Prioritization

Risk is prioritized based on cloud asset exposure and the sensitivity of the data it stores, along with application context such as base image risk, IaC misconfigurations, identity exposure, and sensitive data access. Runtime context further enhances prioritization by identifying which risks are reachable in production so teams focus on truly exploitable risk.



AI-Driven Remediation

Remediation is accelerated with AI-generated fixes for security issues on deployed cloud assets, including automated guidance and code-level fixes for vulnerabilities, misconfigurations, and cloud alerts. This allows teams to quickly validate findings and resolve risks directly in source code, preventing teams from repeatedly fixing the same issue.

About Orca

Orca Security provides a unified cloud security platform that helps organizations identify, prioritize, and remediate risk across cloud environments, applications, and AI. Powered by patented SideScanning™ technology, Orca combines complete visibility with deep context across code, cloud, and runtime, enabling teams to focus on exploitable risk and move from observation to action.

Learn more at https://orca.security.

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