SOLUTION BRIEF

CLOUD SECURITY WITH ORCA

Everyone is a builder. Orca keeps them building.

THE CHALLENGE:

Cloud Complexity Is Outgrowing Security's Ability to Secure It

Cloud environments span more providers, services, and vulnerabilities every year. Vulnerability volume is climbing rapidly, with over 45,000 new vulnerabilities logged in the National Vulnerability Database between January and late July 2026 alone, roughly matching the full-year 2025 total. Further, AI-generated code introduces runtime security violations at nearly 2x the rate of human-written code (University of Texas at Arlington and NJIT, 2026).

Even when risk is found, most of it goes unaddressed. Security teams face thousands of alerts a day but investigate only about 4% of them due to disconnected tools and workflows, resulting in a confirmed fix for less than 1%. The teams tasked with keeping up are flat or shrinking, with more than half of CISOs describing their team as understaffed. The result is that even correctly flagged critical findings sit unresolved for an average of 128 days, and only 26% of known exploitable vulnerabilities were remediated in 2025.

THE SOLUTION:

Security for the Companies That Build in the Cloud

Orca unifies security across cloud, code, AI, and runtime into a single platform, powered by patented Agentless SideScanning™ technology, with a lightweight eBPF Sensor available for teams that need it. Security teams get complete visibility throughout their environment, context that powers every decision, and fixes that adapt to how their team already works.

- ✓ **Complete Visibility:** Orca sees every workload, identity, data store, and line of code across your multi-cloud and AI environment the moment it exists, agentlessly, with nothing new to deploy as your environment grows.
- ✓ **Context That Powers Decisions:** Every finding carries a risk score and the interconnected reasoning throughout your cloud, code, and AI, including reachability, exploitability, attack paths, and more, not just a severity label, updating automatically as your environment changes.
- ✓ **Security That Fits the Way You Work:** Findings route directly into the tools and workflows your team already uses, with pre-configured and customizable / AI Agents and automations for defined scenarios. No new dashboard and no manual handoff.

15min

15 min to full on-boarding across your environment

20,000

Up to 20,000 related alerts addressed by a single patch (Blue Yonder)

$1.2M

$1.2M annual operating savings and 198% ROI (TAG Cyber, 2026)

> ***As a CIO, I need security solutions that align with the pace and complexity of our cloud operations. Orca has been a game-changer—giving us instant, deep visibility. It empowers our team to proactively manage risk, stay compliant, and support the business with confidence. Orca helps us move faster, safer."***

RENIER HUGO
Takealot Group CIO

COPYRIGHT 2026 ORCA SECURITY. ALL RIGHTS RESERVED

How Orca Secures the Cloud

SideScanning™: Orca's patented, agentless technology reads workload data directly from the cloud provider's block runtime storage layer, out-of-band and read-only, so full deployment takes minutes instead of the weeks or months agent rollouts typically require, with zero performance impact on systems.

Unified Data Model: Cloud, identity, workload, data, code, and AI context all live in one graph instead of siloed tools. A vulnerable workload, an overprivileged identity, an exposed secret, and a misconfigured data store aren't four separate alerts in four separate tools. Orca connects them into the attack paths they create together, so teams see the real risk, not just the individual findings.

Dynamic Risk Scoring: Every finding is scored on reachability, exploitability, and blast radius across the full attack path, not a static CVSS label, with the full reasoning behind the score shown alongside it, not just the number. The score updates automatically the moment the environment changes, so a "critical" finding doesn't stay critical after it's patched or isolated.

Orca AI Agent Pod: Pre-built Core Agents apply security expertise across your cloud estate, using the full context of the Orca Platform to act on findings, not just report them.

- **Blue Pod:** Investigates threats and findings to separate real risk from false positives.
- **Red Pod:** Validates what attackers could actually exploit across your attack surface.
- **Green Pod:** Turns findings into fixes and keeps compliance on track.
- **Custom Agents**: Automate your team's workflows from Orca templates or from scratch.

Orca AI: A full suite of AI tools built for security teams. Native MCP support connects Orca's context into the tools your team already uses. AI Code Fix drafts remediations and enables a one-click pull request, and a natural language AI assistant lets anyone search and investigate across the environment.

Orca Sensor: An optional, lightweight eBPF sensor added on top of the agentless foundation for teams that need real-time, in-workload detection, so runtime alerts inherit full cloud, identity, and code context.

Cloud, Code, & AI Security — One CNAPP

- ✓ CSPM
- ✓ CIEM
- ✓ CWPP
- ✓ KSPM & Container
- ✓ API
- ✓ Compliance
- ✓ DSPM
- ✓ AppSec
- ✓ ASM
- ✓ Vulnerability Management
- ✓ CDR
- ✓ AI Security

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 orca.security.

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

COPYRIGHT 2026 ORCA SECURITY. ALL RIGHTS RESERVED