orca security

EXECUTIVE BRIEF

Cloud Security in a CNAPP

Benefits of Agentless CNAPPs

- ✓ Reduce the chance of misconfigurations, mistakes, or security mismanagement of cloud-native applications.
- ✓ Reduce the number of tools and vendors involved in the CI/CD pipeline.
- ✓ Reduce the complexity and costs associated with creating secure and compliant cloud-native applications.
- ✓ Allow security departments to understand attack paths based on relationships—security vulnerabilities, misconfigurations, permissions, exposed secrets—that would enable an attacker to target an application.
- ✓ Bi-directionally link development and operations visibility and insight into risk analysis to improve the overall enterprise security posture.

Simplified cloud security and compliance, and contextual visibility into misconfigurations, workloads, and identities

The Cloud Native Application Protection Platform (CNAPP) is an emerging cloud security category that simplifies cloud security by combining the capabilities of tools such as **Cloud Security Posture Management** (CSPM), **Cloud Workload Protection Platforms** (CWPP), and **Cloud Infrastructure Entitlement Management** (CIEM) in one platform.

Instead of siloed views, CNAPP technology provides full coverage and visibility into cloud estates and can detect security and compliance risks across the tech stack, including cloud configuration, workload, and identity. Furthermore, CNAPPs can incorporate some 'shift-left' capabilities to identify risk earlier in the development lifecycle. By combining vulnerabilities, context, and relationships, CNAPPs provide a holistic view of risks, recognizing how seemingly unrelated low severity risks can be combined to create dangerous attack vectors.

When the CNAPP is agentless, it solves a number of challenges that security teams are facing with current security approaches, including:

- Gaps in coverage from traditional security tools that require agents on all workloads
- Difficulties in deploying and maintaining scanners and agents
- Alert fatigue caused by ineffective risk prioritization
- Multiple disparate tools create overhead for security teams

Choose a CNAPP that's right for you

Get the CNAPP Buyer's Guide: 5 Considerations for Evaluating Cloud-Native Application Protection Platforms:

Get the guide

orca security

CNAPP Buyer's Guide

5 Considerations for Evaluating Cloud-Native Application Protection Platforms

Orca Detects and Prioritizes these Top Risks

- ✓ Vulnerabilities
- ✓ Misconfigurations
- ✓ Malware
- ✓ Misplaced Sensitive Data
- ✓ Lateral Movement Risk
- ✓ Authentication Risk

Trusted by Organizations Across the Globe

fiverr.
Lemonade
unity
BeyondTrust
LiveOakBank
databricks
druva
Robinhood
Fyber
Rapyd
paidy

How Orca Transforms Cloud Security

Orca Security is the pioneer in securing multi-cloud environments, delivering CNAPP capabilities with its agentless, multi-faceted approach to cloud security and compliance, in one platform.

The Orca Platform combines cloud workload and configuration intelligence in a unified data model and a single pane of glass, allowing the holistic insight that you just can't get with separate solutions. By seeing the bigger picture, Orca is able to pinpoint exactly which issues are critical and which ones are not, as well as recognize when seemingly unrelated issues can be combined to create dangerous attack paths.

SideScanning™ Technology

Orca leverages cloud configuration and workload data to build a fully contextualized asset inventory and perform a holistic security assessment of your entire cloud estate. Orca's patent-pending SideScanning™ technology collects data, with read-only access, from the workloads' runtime block storage and retrieves cloud configuration metadata via APIs. This allows Orca to detect vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and unsecured PII—all without any performance impact on your workloads.

Context-Aware Security

Orca's context engine combines the intelligence gathered from deep inside workloads including the workload's host configurations (e.g., running services, network configurations) and cloud configuration details (e.g., IAM roles, VPCs, security groups) to build a unified data model. This powerful approach enables Orca to build a visual map of your cloud estate, including interconnectivity between assets. This preemptive view of your cloud attack surface immediately surfaces the critical security issues and their root cause without overwhelming your security team with thousands of meaningless alerts.

Automated Cloud Compliance

With its agentless approach and ability to replace multiple security tools, Orca allows teams to maintain continuous compliance, with over 40 regulatory and industry frameworks and key CIS benchmarks supported. These include key regulatory mandates, such as PCI-DSS, SOC 2, PSD2, GDPR, NIST-800-53, ISO 27001, HIPAA, and more. With Orca's built-in, customizable compliance templates to meet your specific needs, your team can focus on audit readiness and compliance requirements when it matters most.

orca security

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