Orca Security FAQ

What does Orca Security do?

Orca Security offers a radical new, agentless approach to cloud security and compliance that provides 100% visibility and coverage of cloud configurations and workloads while eliminating the cost, organizational friction, and performance hits associated with agent-based solutions. By detecting security risks at the cloud infrastructure, OS, application and data layers of your AWS, Azure, and Google Cloud estates, Orca eliminates the need to deploy and maintain multiple tools, such as CSPMs and CWPPs. Leveraging context-aware intelligence, Orca effectively prioritizes the 1% of truly critical risks and discovers dangerous attack paths that would be completely missed by other solutions.

What problems does Orca Security solve?

The Orca platform solves a number of significant problems that exist in current cloud security solutions:

- **Cumbersome deployment:** Installing and maintaining agents on every cloud workload results in performance degradation, organizational friction, and extremely high TCO.
- **Coverage gaps:** Partial deployment of agents causes serious blind spots. On average, we found that less than 50% of assets are covered by agent-based solutions.
- **Performance degradation:** Cloud security solutions based on agents or network scanners have a significant impact on application performance and system resources.
- **Alert fatigue:** Security teams waste valuable time manually sifting through high volume, low-risk alert data which lack prioritization and actionable details, resulting in alert fatigue and missed critical issues.
- **Multiple disparate tools:** With no single pane of glass, overworked security teams face the complexity and heavy administrative burden of managing multiple siloed tools.

What are the benefits of the Orca Security platform?

- **Agentless:** Orca eliminates the gaps in coverage, organizational friction, performance hits, and high operational costs of agent-based solutions.
- **100% coverage and visibility:** Orca provides full-stack visibility and covers all your cloud assets within minutes, even VMs, containers, and serverless, as well as cloud infrastructure resources.
- **Multiple tools in a single platform:** As a CNAPP, Orca includes the core capabilities of CSPM and CWPP solutions, including vulnerability management and compliance management, in a single platform.

- **Effective alert prioritization:** Orca's context-aware engine prioritizes the 1% of alerts that truly matter and need immediate attention.
- **Detect attack paths missed by other solutions:** Unlike legacy solutions, Orca leverages context-aware intelligence to recognize when seemingly unrelated issues can be combined to create dangerous attack paths.
- **Deploy once - secure forever:** Orca automatically detects and monitors new cloud assets as you add them, without requiring any manual updates.
- **Multi-cloud support:** Orca is an enterprise-scalable platform that can secure large multi-cloud estates efficiently and with low-overhead.

Which risks does Orca Security detect?

Orca detects and prioritizes the following risks: vulnerabilities, misconfigurations, malware, misplaced sensitive data, lateral movement risk, and identity and access management (IAM) risk.

What is Orca's SideScanning™ technology?

Orca's patent-pending SideScanning addresses the shortcomings of agent-based solutions by collecting data, with read-only access, from the workloads' runtime block storage out-of-band. By combining this data with cloud configuration metadata retrieved via APIs, Orca has full visibility into every layer of your cloud estate. This new, agentless approach allows Orca to be deployed in minutes and automatically cover new assets as they are added.

Which assets does SideScanning cover?

Orca covers 100% of your cloud infrastructure assets, including VMs, containers, and serverless as well as all cloud infrastructure resources like storage buckets, security groups, VPCs, IAM roles and permissions, KMS keys, and much more. Orca even discovers and monitors idle, paused, and stopped workloads, orphaned systems, and devices that can't support agents.

What is Orca's Context-Aware security?

Whereas traditional solutions consider only one dimension of risk – the severity of the underlying security issue (e.g. CVSS score) – Orca's context engine understands each asset's role within its context and is therefore able to prioritize the truly critical security issues instead of just alerting to all threats found. To determine the priority of an issue, Orca looks at the following three factors: (1) severity of the security issue, (2) accessibility by attackers, (3) business impact of a potential breach. For example, malware found in a powered-off VM should not be prioritized over a malware-infected, internet-facing workload housing a secret key that unlocks sensitive data in an adjacent workload. By seeing the bigger picture, Orca is able to prioritize the alerts that are most critical to your security posture.

Does Orca provide a visual representation of cloud assets?

Yes. For each alert, Orca provides an attack vector graph showing the respective asset in context, what asset type it is, whether it is public facing, if there is lateral movement risk, etc.

Does Orca help organizations achieve cloud compliance?

Yes, Orca supports regulatory compliance by alerting to threats ranging from vulnerabilities and malware, to file integrity and leaked/weak passwords. Orca supports compliance for 35+ key frameworks and CIS benchmarks and provides out-of-the-box compliance templates that can be customized to suit your needs. Orca also detects the presence of sensitive data such as PII and any potential exploitation paths, helping you meet data privacy mandates such as PCI-DSS, GDPR, CCPA, and HIPAA.

What is Orca's Automation and Customization feature?

With Orca's Automation and Customization feature, security teams can query cloud estate data to access essential intelligence and automatically assign cloud security issues to specific teams for more efficient triage, remediation, and compliance management. Companies can utilize any of the 600+ out-of-the-box query templates or write their own custom queries. Queries can be run as one-offs or as alerts, and can be integrated with notification systems such as email, Slack, OpsGenie, or PagerDuty as well as ticketing systems such as Jira or ServiceNow.

Does Orca support multi-cloud configurations?

Yes, Orca supports multi-cloud estates from IaaS providers AWS, Azure, and Google Cloud, allowing you to manage your cloud security and compliance from a single platform.

How long does it take to deploy Orca Security?

Orca Security deploys in minutes - not months - because there are no agents to install and no opcode runs within your cloud environment. Setting up Orca is a simple three step process:

1. Log into your cloud service provider
2. Create an IAM role with policies for Orca
3. Connect Orca to begin SideScanning

How can I get a demo of Orca Security?

Contact us for a demo at: https://orca.security/demo/

orca security

Connect your first cloud account in minutes and see for yourself: Visit orca.security