Orca SideScanning™ Technical Brief

How Orca's Patented Technology Powers Modern Agentless Cloud Security

Table Of Contents

Executive Summary 1

Why Legacy and Siloed Security Solutions Fail in the Cloud 2

Cloud Workload Protection Platforms 2

Cloud Security Posture Management Solutions 3

Agent-Based Vulnerability Scanners 3

Authenticated Network-Based Vulnerability Scanners 4

Unauthenticated Network-Based Vulnerability Scanners 4

Introducing SideScanning™ — Orca's Revolutionary Approach to Securing Your Entire Cloud Estate 5

Overview 5

Like an MRI for Your Cloud Estate 6

No Impact on Workloads or DevOps 6

How SideScanning Works 7

Orca Deployment 7

Block Storage Snapshots 8

Asset Discovery and Enumeration 8

Key Part of Orca's Unified Data Model 9

Control Plane Analysis 10

Data Plane Analysis 11

At-Risk Sensitive Data Detection 15

Container Scanning 16

Information Integration, Analysis, and Reporting 17

Summary 19

Revolutionary SideScanning 19

Enterprise-Ready, Multi-Cloud Security 20

About Orca Security 21

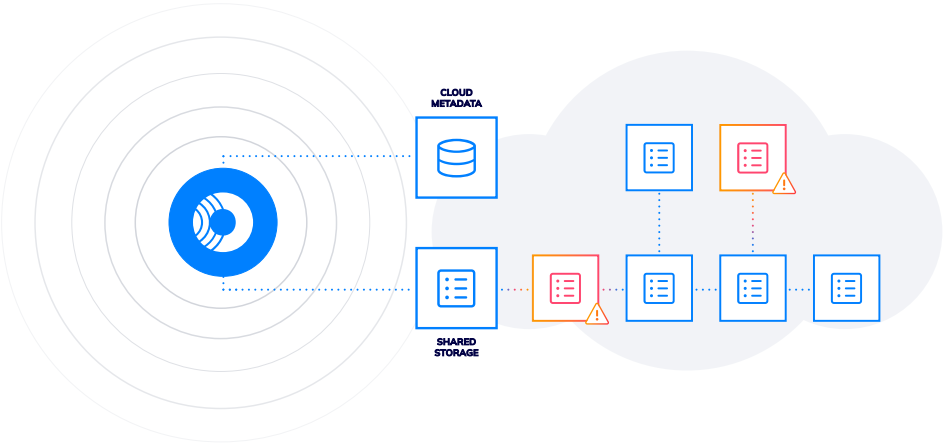
Trusted by Organizations Across the Globe 21

Executive Summary

Last-generation security tools, such as host-based and network vulnerability scanners, were not designed for the cloud, but for the slow-changing legacy world of yesterday. They rely on deployment modes such as host-based agents and network access—outdated operational models that are completely at odds with the core “speed and agility” principles of cloud computing.

Even newer cloud security solutions, such as cloud workload protection platforms (CWPP) and cloud security posture management solutions (CSPM), suffer from similar challenges. Organizations attempting to use legacy formats and point solutions in the cloud quickly realize their limitations such as complex deployment, time-consuming management, incomplete and shallow coverage of workloads, performance degradation, and high total cost of ownership (TCO).

Orca Security introduces a revolutionary single platform solution for cloud security that covers all assets across your cloud estate, delivers prioritized alerts in context, and helps you meet compliance mandates. Orca is the only vendor that effectively prioritizes alerts using a holistic unified data model that combines workload data (vulnerabilities, misconfigurations, malware, file integrity monitoring), threat intelligence, and environmental context (accessibility, potential business impact and more). Built specifically to help secure AWS, Azure, Google Cloud, Kubernetes, Oracle Cloud and Alibaba Cloud environments, Orca Cloud Security Platform dramatically simplifies security deployment and management, closes visibility gaps, eliminates performance degradation caused by agents, and lowers TCO.



ORCA SIDESCANNING READS WORKLOADS THROUGH THE CLOUD PROVIDERS’ SHARED STORAGE

Why Legacy and Siloed Security Solutions Fail in the Cloud

IT infrastructure has undergone many changes in a relatively short period of time. On-premises servers networked with monolithic storage systems have given way to virtual and ephemeral cloud compute instances, containers, and serverless functions networked with infinitely scalable storage and other cloud services. A number of security solutions, such as CWPP and CSPM tools, have become available as vendors and cloud providers attempt to fill ever-widening cloud security gaps. In addition, some legacy vulnerability scanning solutions have been updated for cloud deployment.

Even though some vendors have now started offering an 'agentless' option in addition to their agent-based solution, they often have hidden limitations and only increase complexity rather than simplify deployment. Unlike the Orca Cloud Security Platform, these solutions were not purpose-built to be agentless, and to be effective, they still require agents to be installed on many cloud assets.

Unfortunately, these solutions suffer many of the same shortcomings as their physical data center predecessors. At Orca Security, we believe that strictly relying on agent-based solutions and outdated scanning technologies to secure modern cloud environments is fundamentally flawed. Below we list some of the shortcomings and weaknesses of these solutions when deployed in the cloud.

⚠ Cloud Workload Protection Platforms

Cloud Workload Protection Platforms (CWPP) were initially developed directly from legacy on-premises host protection solutions and then adapted to be more cloud-friendly. They require installation of an agent on each and every VM or compute instance to function, and therefore simply cannot scale to meet the operational and security requirements of modern dynamic cloud environments. Multiple agents must be installed to support different operating systems and versions, and agents must remain connected to the backend or the public internet, leaving them vulnerable. Attempting to use agent-based solutions to monitor containers and serverless functions is even more problematic.

What's more, in the fast-paced world of DevOps, developers don't want to waste time installing agents on all hosts. And once they are installed, agents must be continually updated with the latest virus signatures and patches, leading to a never-ending maintenance cycle with high TCO.

⚠ Cloud Security Posture Management Solutions

As organizations began embracing cloud-first initiatives and moving mission-critical workloads to the cloud, security vendors took notice. The operational overhead and security risks associated with agent-based security tools were critical issues that needed to be addressed. Cloud Security Posture Management (CSPM) solutions were developed to scan cloud accounts and services for compliance and misconfiguration issues while leaving cumbersome agents behind.

But rather than scanning deeply inside of cloud workloads, CSPM tools only analyze the cloud infrastructure layer for weaknesses. They can't detect critical risks such as vulnerabilities, malware, and misconfigurations within the workloads themselves. Organizations are often forced to deploy agent-based solutions alongside CSPM tools to help fill security gaps. Unfortunately, multiple siloed tools can overwhelm security teams with meaningless alerts that lack context and delay remediation efforts. Clearly, CSPM solutions are not enough, even when deployed alongside agent-based CWPP solutions.

⚠ Agent-Based Vulnerability Scanners

Many vulnerability scanning solutions have been retooled for the cloud in attempts to extend their lifespans. They typically fall into three categories, the first of which are known as agent-based vulnerability scanners. But again, annoyances suffered by their on-premises customers are only amplified in the cloud. They are difficult to install and maintain, and their visibility is limited to the subset of assets that are known, accessible, and capable of hosting an agent.

Orca's customer engagements have revealed that the average organization relying on agent-based cloud security lacks security visibility into at least 50% of its cloud infrastructure footprint. This is because many assets are either difficult to instrument or won't accept agents. Also, the continuous updates that agents require can create unacceptable DevOps friction and high TCO.

⚠ Authenticated Network-Based Vulnerability Scanners

Authenticated vulnerability scanners are relatively uncommon these days as they are expensive to use and maintain. They attempt to access their target hosts over the network using remote protocols such as SSH or RDP. While authenticated scanners can successfully discover potential vulnerabilities, they require a privileged account on each scanned host. Creation and maintenance of multiple privileged accounts creates multiple opportunities for abuse by attackers. Furthermore, authenticated scans use significant system resources and require open ports, which also pose a security risk.

⚠ Unauthenticated Network-Based Vulnerability Scanners

An unauthenticated scanner only examines publicly visible information. It can't provide detailed information about assets. In addition, an unauthenticated scan can easily miss critical assets and vulnerabilities. For example, consider that you maintain a website named 'mydomain.com/email_campaign' that isn't connected to your main website. The website won't be scanned unless the unauthenticated scanner is manually configured to do so, but no organization can ensure manual setup for a large number of exceptions. This leaves many organizations exposed to vulnerabilities in areas where unauthenticated scanners simply can't reach. Additionally, unauthenticated scanners often get stuck where an attacker would not. For example, a CAPTCHA can easily prevent any automatic mechanism (including scanners) from registering. However, a CAPTCHA can be bypassed by an attacker who could register as a user and take advantage of a vulnerability missed by the scanner.

Unfortunately, all of these legacy scanning solutions fall short in the cloud.

Introducing SideScanning™— Orca's Revolutionary Approach to Securing Your Entire Cloud Estate

Overview

Orca's patented SideScanning™ technology has finally fixed cloud security. Using a completely agentless approach, SideScanning analyzes cloud workloads via their runtime block storage layer. By combining workload runtime data with metadata gathered from cloud service provider APIs, Orca is able to visualize your entire cloud estate to put risk and threats in the proper context for your unique environment. For example, if you have 100 machines running in the cloud that need to be updated to patch a critical vulnerability, but one of them has a database behind it that contains personally identifiable information (PII), Orca will alert you to the imminent compromise so you can update that machine first.

Orca Security uses a quick, one-time integration into your Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Oracle Cloud, or Alibaba Cloud environments, and within minutes, scans the asset configurations, network layout, and security settings of your entire cloud environment. At the same time, Orca reads security-related data from your VMs, containers, Kubernetes, databases, data stores, managed services, identities, APIs, AI models, and serverless functions. It then analyzes the data and builds a complete inventory and map of your cloud estate. Next, it automatically assesses the security state of assets across your full cloud stack, including the infrastructure, OS, application, and data layers.

The cloud estate refers to your cloud-based assets, including running, stopped, paused and idle workloads of all types, related components, and configuration settings. Examples include VMs, containers, object stores, load balancers, IAM configurations, serverless functions and more.

Like an MRI for Your Cloud Estate

A good analogy for SideScanning is a medical MRI scanner. Instead of using needles and scalpels to conduct invasive exploratory surgery, the MRI machine diagnoses health issues through non-invasive scanning to obtain a detailed picture of all organs and tissues. The patient is never actually touched by the physician during the procedure.

SideScanning is similar in that it visualizes all cloud assets and connectivity to build a complete model of your cloud environment. It then uses this model to determine risk in the proper context without affecting cloud assets or their functionality in any way.

No Impact on Workloads or DevOps

Orca SideScanning doesn't run on your workloads so it can examine 100% of your cloud environment without impacting your workload performance. And since the SideScanning process doesn't use agents that require installation, it can be deployed at any time and won't impact your IT or DevOps teams.

How SideScanning Works

Orca Deployment

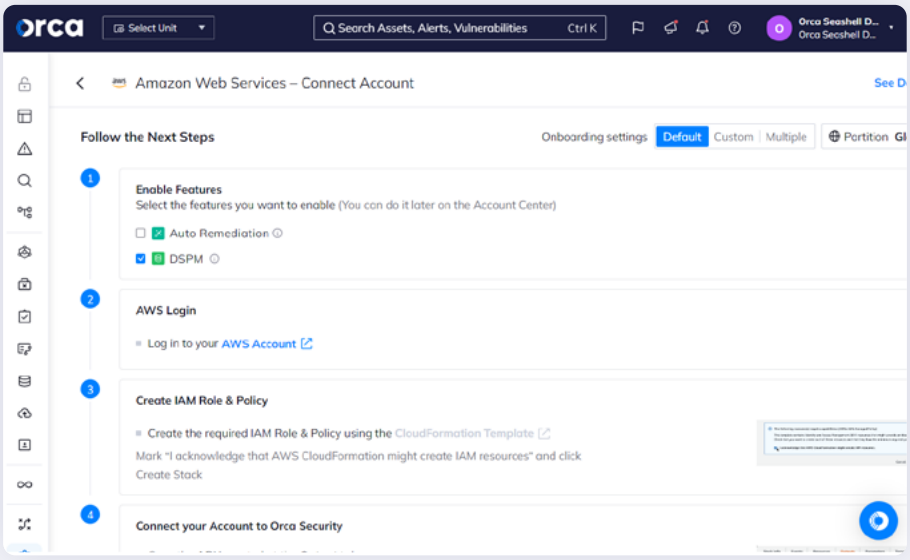
Orca customers can choose from two deployment modes; default Software-as-a-Service (SaaS) mode, or in-account (Orca Pod) mode. For simplicity, all scenarios and explanations below refer to our default SaaS deployment mode, and we use AWS cloud terminology throughout the rest of this document. Please note that similar concepts apply to Microsoft Azure, Google Cloud, Oracle Cloud, and Alibaba Cloud environments.

Before the SideScanning process can begin, customers must complete a one-time, three-step (with an optional fourth step) onboarding process that takes just a few minutes. In the example below, we describe the steps to connect to AWS:

1. Login to your AWS account.
2. Create the required identity and access management (IAM) role and policy.

   Note: You provide Orca with a role to establish trust between your cloud account and Orca's production account. The role has a few permissions, the most important being read-only permissions to the block storage layer. For AWS, the process is encapsulated within a CloudFormation template, which means that an administrator simply clicks once to open the template, and then once more to apply it.
3. Copy and paste the resulting Amazon Resource Name (ARN) into the Orca user interface.
4. If you would like to use Auto Remediation, create the required resources using the CloudFormation template.

Customers with more than one account have the option to onboard multiple AWS accounts in a simple automated process. Now the SideScanning process can begin.



ORCA ONBOARDING STEPS FOR AWS

Block Storage Snapshots

The Orca SideScanning process begins by leveraging the snapshot function to create snapshots of the block storage of all machines in your environment. Orca snapshots multiple volumes simultaneously for deep and consistent visibility.

> **Note:** These snapshots can only be accessed from your account for security. Since Orca uses read-only access credentials, the SideScanning process can't make any changes to your workloads or infrastructure, and won't make any changes to or impact your runtime environment.

Orca takes the security and confidentiality of your information seriously and implements a number of best practices to ensure that your data remains secure:

- Any sensitive data that's been discovered and triggers an alert, such as PII at risk, is masked before the alert is displayed in your Orca dashboard.
- During the SideScanning process, all customer data is handled securely complying with ISO-certified techniques and procedures.
- As Orca creates snapshots, they are simultaneously tagged for deletion as soon as the SideScanning process is complete.

Asset Discovery and Enumeration

Orca scans snapshots created for the SideScanning process to discover and enumerate all cloud assets including:

- Virtual machines
- Containers
- Kubernetes
- Serverless functions
- Cloud storage
- Databases
- VPCs
- Cryptographic keys
- Secrets
- Images
- Managed Services
- Load balancers
- Network delivery
- Security groups
- Users
- Roles
- Policies
- AI Models

For a full list for each cloud platform, please view the Orca technical documentation.

After all assets have been identified and mapped, the SideScanning process begins an in-depth analysis of the cloud control plane and the data plane to enrich these initial findings with more detailed risk information and context.

Key Part of Orca's Unified Data Model

SideScanning is one of the main data sources for the Orca Platform. The platform also consumes data from several other sources and centralizes all of this information in a Unified Data Model. Orca pulls in data from:

- SideScanning (deep contextual cloud workload data)
- Cloud control plane (data from cloud provider APIs)
- CI/CD scans (scan results from container images, Infrastructure-as-Code, and registries scanning)
- Authentication (Users' data enrichment from different IdPs)
- Cloud events and audit logs (DNS feeds, cloud provider audit logs, etc.)
- Network probing (external attack surface enrichment for Internet-facing assets)

All of this data is used to empower your teams to achieve desired security outcomes through our Platform.

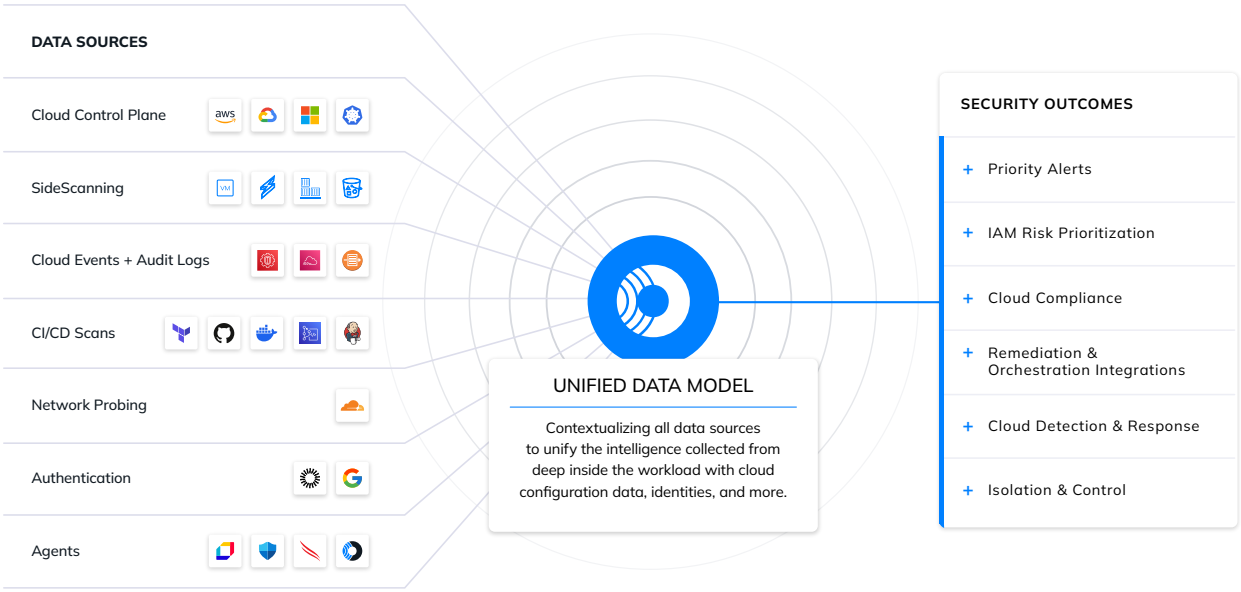
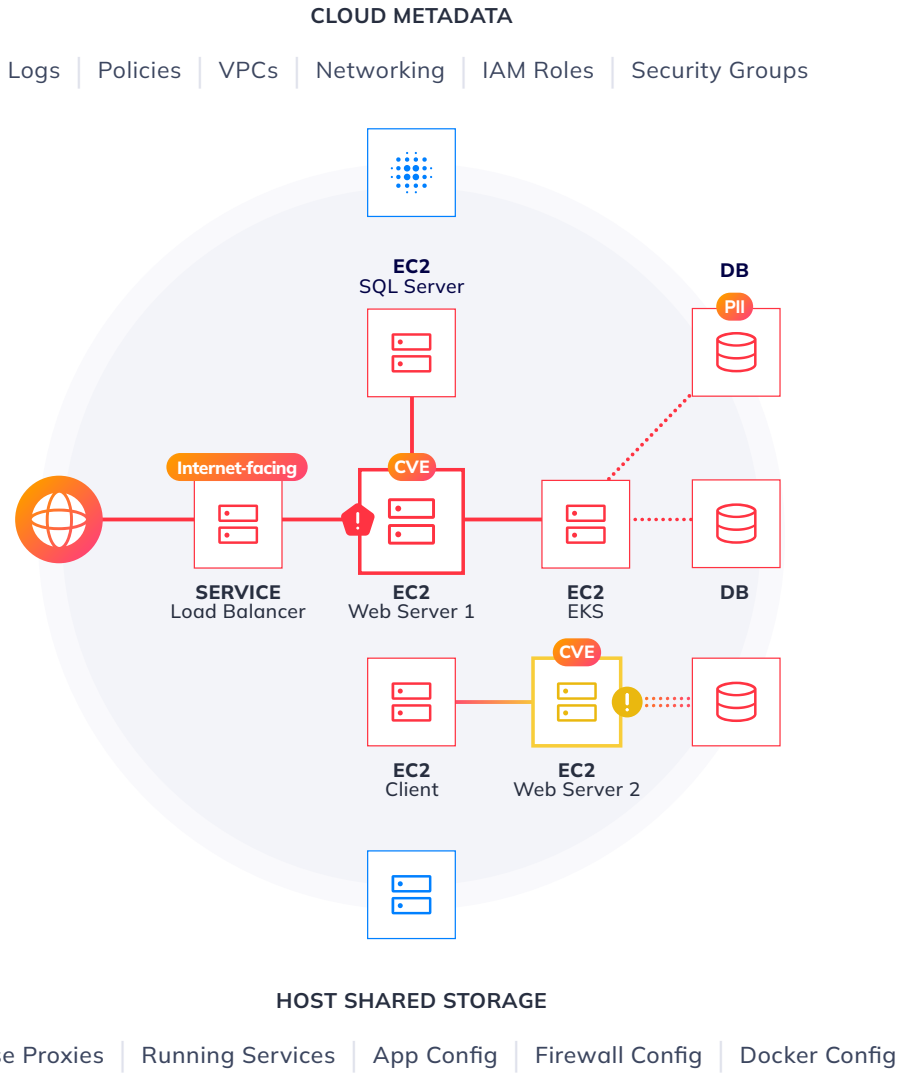


DIAGRAM OF ORCA'S UNIFIED DATA MODEL

Control Plane Analysis

Complementary to the SideScanning process, Orca also discovers and examines a wide range of cloud provider services via integration with cloud provider APIs, and maps their relationships to all assets. Orca uses this information to perform an initial risk assessment of your cloud environment, and to build a complete infrastructure map that will act as a guide during data plane analysis.



ORCA USES SNAPSHOTS OF SHARED BLOCK STORAGE AND CLOUD METADATA TO CREATE A DETAILED CONTEXT MAP OF YOUR UNIQUE CLOUD ENVIRONMENT

Data Plane Analysis

This is where SideScanning does the heavy lifting. For data plane analysis, Orca deploys a dedicated “Orca scanner”—typically an ephemeral Amazon EC2 Spot instance—within Orca’s cloud account. The Orca scanner inventories and organizes the snapshot volumes and then mounts each snapshot in a way that simulates your production environment. Next, Orca subjects each snapshot to intensive inspection and analysis across essential categories of discovery to extract the detailed contextual metadata that finally brings your risk landscape into sharp focus.

Vulnerability Scanning

Orca extracts all OS packages, libraries, and program language libraries such as Java archives, Python packages, Go modules, Ruby gems, PHP packages, and Node.js modules. Next, Orca attempts to match library information and other identifying characteristics with known vulnerabilities in its vulnerability database. Orca’s comprehensive vulnerability database contains information aggregated from a variety of industry-recognized vulnerability sources including:

- National Vulnerability Database (NVD)
- US-CERT
- OVAL – Red Hat, Oracle Linux, Debian, Ubuntu, SUSE
- Japan Vulnerability Notes (JVN)
- Alpine secdb
- Amazon ALAS
- Red Hat Security Advisories
- Debian Security Bug Tracker
- Exploit Database
- JPCERT
- WPVulnDB
- Node.js Security Working Group
- Ruby Advisory Database
- PHP Security Advisories Database
- RustSec Advisory Database
- Microsoft MSRC, KB
- Kubernetes security announcements
- Drupal security advisories

Misconfiguration Detection

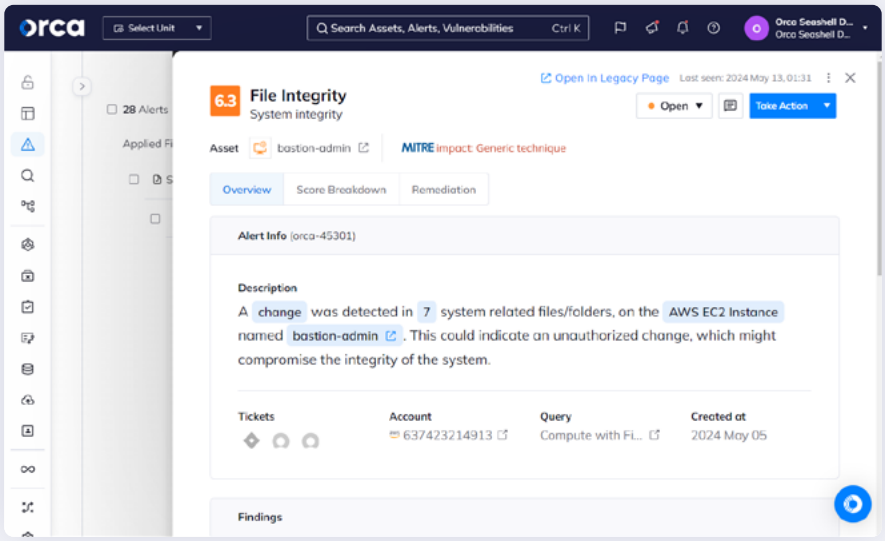
During misconfiguration detection, SideScanning examines application-specific and OS-specific configurations for Apache, Nginx, SSH, Ubuntu Linux, Red Hat Linux, Amazon Linux, MS Windows, and more. Orca combines this with information collected previously during device enumeration, such as a machine’s users, services, and password hashes. It’s important to use this data when calculating risk as some packages might only be vulnerable when deployed in specific configurations. Orca also uses these configuration-specific details to augment vulnerability scanning results.

After taking snapshots, Orca only uses cloud service provider APIs to access cloud account configuration data. No other customer resources such as disk or RAM are used during the assessment process.

Orca examines the resulting configuration metadata and removes any sensitive information before encryption and transfer to its secure environment for further analysis. Now Orca compares the configuration metadata against CIS and other benchmarks to surface any cloud asset misconfigurations.

File Integrity Monitoring

SideScanning also implements file integrity monitoring (FIM) to monitor a set of critical files in your Linux and Windows workloads for any baseline drift. FIM is important for compliance with certain regulations, such as PCI-DSS. Orca discovers and classifies any changes or drift from baseline configurations and provides you with remediation information.



ORCA SHOWS ALL ASSET INFORMATION, INCLUDING FILE INTEGRITY

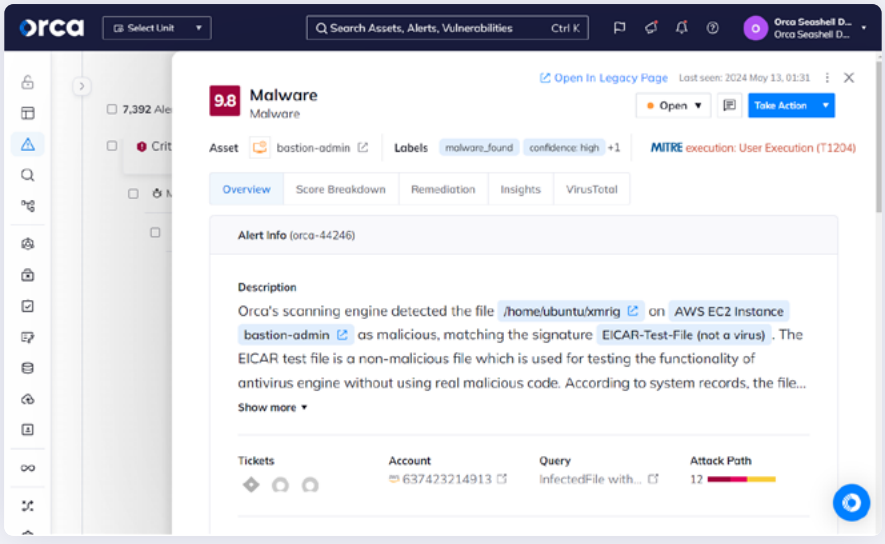
Compliance Monitoring

Whether your cloud environment is subject to regulatory frameworks, or you prefer to define and benchmark against your own standards, SideScanning can alert you to potential compliance violations and risk across your entire cloud estate. Choose from more than 160 industry and regulatory framework templates, which you can use out-of-the-box, or modify as needed. Compliance scanning and reporting can be scheduled to provide regular updates and alerts to your audit teams.

Anti-Malware Scanning

The Orca scanner detects both known and unknown threats by performing a deep scan across the entire file system using a sophisticated third-party malware detection engine that performs both heuristic and signature-based detection. Orca's heuristic-based detection enables discovery of polymorphic malware, something that security solutions that only compare malware hashes can't do.

Anti-malware scanning is performed entirely on the Orca side, so it won't affect your production workloads. Since the Orca scanner runs on an Orca host, it can't be tampered with by any malware that might be running on the machine being scanned. This enables Orca to detect advanced threats, such as rootkits, that might otherwise evade agent-based scanners.



ORCA MALWARE ALERT

Since Orca's scanning process is read-only, it can't be affected by malware running on an infected cloud workload or service. We never run a potentially malicious application, we just observe it from a different machine. This allows Orca to discover threats, such as rootkits, that are otherwise invisible to agent-based solutions.

This also means that Orca can scale compute resources as needed to support the SideScanning process without affecting your cloud provider billing. And, unlike agent-based solutions, Orca isn't limited by CPU size and memory allocated to customer workload hosts.

Attack Path Analysis

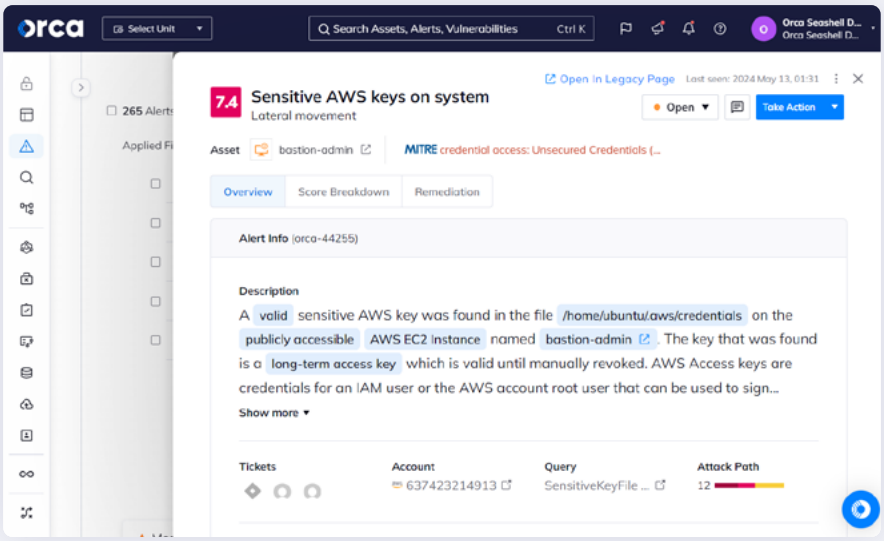
Attackers often need to compromise multiple assets in your cloud environment before they can reach their end goal. To accomplish this, they establish an initial foothold and then scan neighboring assets for exposed keys, unencrypted passwords, and other information that they can use to move laterally. When scanning your cloud estate, Orca not only looks at individual risks, but also looks at your environment just like an attacker does. SideScanning discovers relationships and connections between assets and looks for accessible keys, passwords, vulnerabilities, and more, that an actual attacker might be able to use to move laterally. When Orca detects an issue, it displays prioritized alerts and enumerates all findings in detailed risk reports.

Key Discovery

Orca scans each machine's filesystem for private keys and creates hashes of all discovered keys. Then Orca scans all other assets for authorized public key configurations with matching hashes. Further analysis allows Orca to provide detailed key-related information such as:

- Paths to insecurely stored keys
- Identities of assets that can be accessed with exposed keys
- User accounts and privileges stored on assets

SideScanning also discovers any remote access keys including cloud service provider keys, SSH keys, and more, that might allow attackers to access additional sensitive resources.



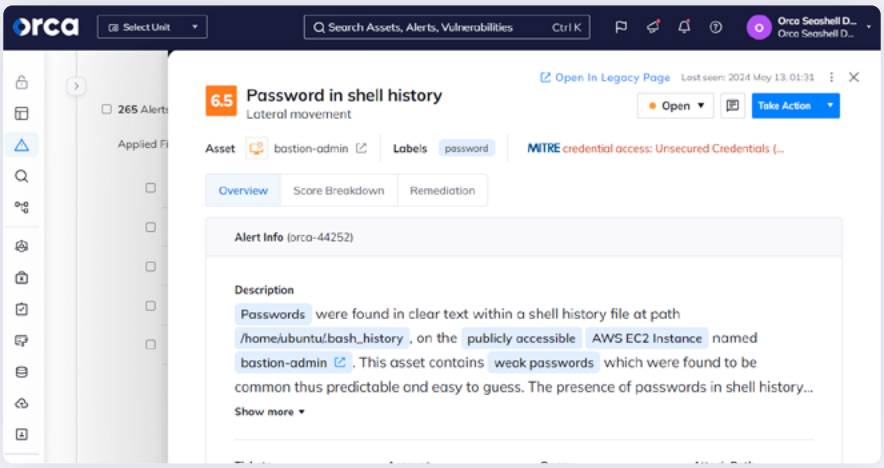
ORCA HAS FOUND SENSITIVE AWS KEYS THAT COULD BE ABUSED BY ATTACKERS

For keys capable of accessing multiple machines, such as SSH keys, Orca discovers and enumerates all additional accessible workloads. For example, Orca might report: “This machine has a private key stored in an unprotected place. The key provides root access to these other machines where the matching public key is installed.” If SideScanning encounters keys that are no longer useful, such as test keys, Orca checks the validity of the keys and notes their permissions before sending a high priority alert. This helps to avoid unnecessary false positives. Keys are never shared outside of the Orca scanner. For example, when examining SSH keys, Orca extracts only the key digest, or hash. For AWS keys, Orca extracts only the access key ID, which is not confidential, along with accessible permissions. The key digest enables Orca to compare public and private keys, and to indicate where lateral movement is not only possible but is easy to accomplish.

Discover Weak and Leaked Passwords

Poor password hygiene is detrimental to your organization’s security posture and encompasses commonly used passwords, complex passwords that are reused across multiple applications and services, and highly secure passwords that have been leaked.

SideScanning inspects all workloads to discover weak or encrypted passwords, including IT scripts containing passwords that an attacker might be able to leverage when moving laterally. For example, let’s suppose that SideScanning discovers a weak, unprotected password stored on a machine. Orca will attempt to match the weak password to commonly used passwords and to passwords in leaked password databases.



ORCA LATERAL MOVEMENT RISK ALERT SHOWING LEAKED PASSWORDS STORED IN SHELL HISTORY OF INTERNET-FACING ASSET AND ASSET ROLE DETAILS

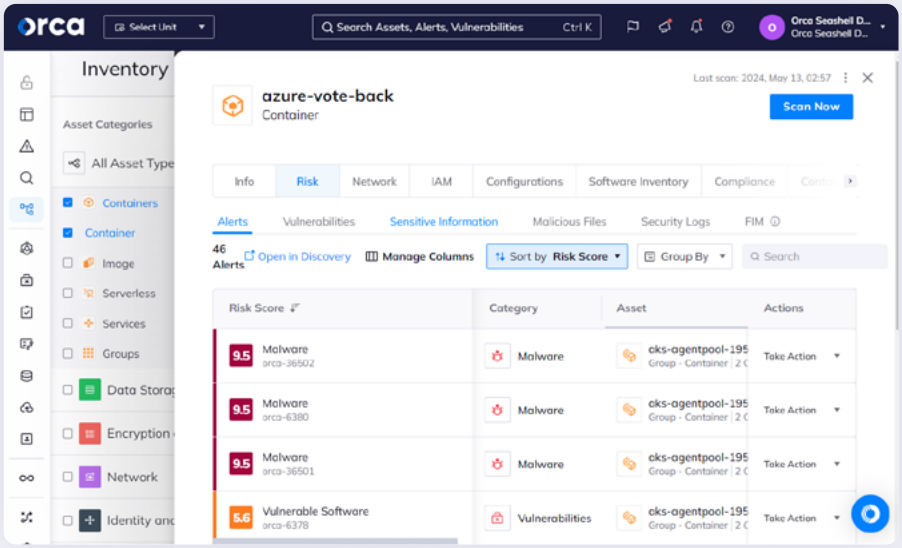
Orca also performs an offline brute force attack to determine how easily a threat actor could break into sensitive accounts. For example, if a user's personal email has been compromised, Orca looks for similar names in published password lists and attempts a brute force login to the machine being tested. Orca makes note of the stored password along with a corresponding pointer.

Like keys, passwords are never shared outside of the Orca scanner.

In addition, Orca highlights bugs and other configuration risks that might only be exploitable from internal machines, yet could facilitate an attacker's lateral movement.

At-Risk Sensitive Data Detection

SideScanning examines your cloud estate to discover PII, including email addresses, physical addresses, social security numbers (SSN), and credit card numbers. SideScanning also searches data repository histories for sensitive information. It's not uncommon for an entire production code repository to be cloned before removing sensitive information, and then forgotten. Orca tags such repositories as risky, noting their location in a vulnerability report. Orca leverages statistical scans and threshold-based heuristics to help reduce false positives. A statistical scan may determine, for example, that a single, random nine-digit number in a file is unlikely to be a real social security number versus a file containing many nine-digit numbers.



EXAMPLE OF ORCA ALERTS ON A CONTAINER

Container Scanning

SideScanning also examines containerized environments, regardless of the orchestration mechanism, Kubernetes or other. When SideScanning encounters a workload that includes containers, it reconstructs the container runtime layered file system and recursively runs the data plane analysis process mentioned above to detect vulnerabilities, misconfigurations, malware, lateral movement risks, sensitive information, etc.

Orca also reads the container's network configuration, using the information to update the contextual map built during control plane analysis. This means that the final map will also include relationships between all discrete and containerized workloads.

SideScanning provides several benefits beyond other container vulnerability scanning approaches:

- **Runtime state scanning** - In addition to container image repositories, Orca also scans the runtime state of the container. This means that Orca can detect deviations from the baseline, including potential compromises of the environment.
- **Orchestration layer agnostic** - Orca covers all container deployments regardless of how they are integrated with the orchestration layer, such as using Kubernetes.

Orca handles native PaaS container environments, such as AWS Fargate, and serverless functions, such as AWS Lambda, in a similar fashion. The major difference being that Orca integrates directly with AWS Fargate/AWS Lambda instead of with the underlying VMs, which generally aren't accessible.

Orca integrates and analyzes the 'bird's eye view' of the control plane and the 'detailed view' of the data plane, and stores the results in a single holistic database, allowing you to view all assets and associated risks in full context without manual data collection or integration.

Information Integration, Analysis, and Reporting

Finally, Orca integrates and analyzes all collected data to produce actionable, context-based alerts and reports. Vulnerabilities are grouped by type, location, and priority so that security engineers and DevOps teams can allocate their time and attention efficiently.

Prioritizing Alerts Using Proper Asset Context

Orca combines findings from different environmental perspectives into a single, unified data model. It takes the asset map from the control plane—where the service meshes and containers talk to each other—and enriches this information with the risk data gathered from workload-deep scanning.

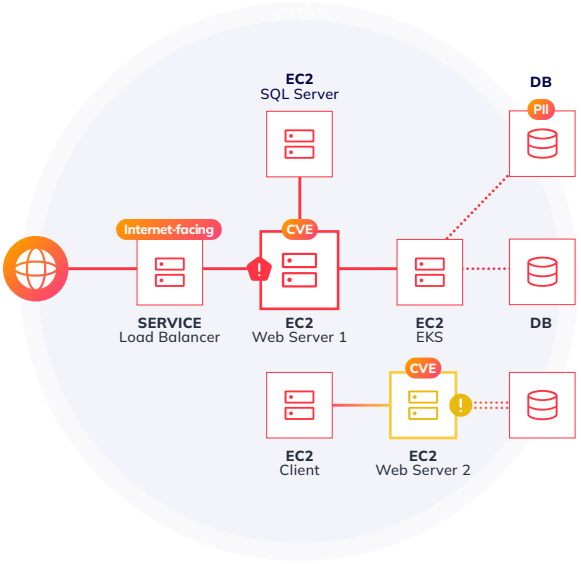
When Orca scans a workload, it notes all services running on it and then overlays the vulnerability data collected during data plane analysis. Orca also determines whether or not the workload is internet-facing and accessible to attackers, which will increase the risk score. All of this information is used to place each asset in the proper context to assess the actual risk.

For example, consider a vulnerability in a web server. Orca will score it as:

- **High risk** if it's connected to the internet, either directly or indirectly via a load balancer or reverse proxy.
- **Medium severity** if it's only accessible internally.
- **Low severity** if it's blocked by a cloud provider security group configuration.

Now let's consider a stopped machine. The machine could have a serious vulnerability, however since it isn't likely to be exploited when the machine isn't running, this will result in a low risk score.

Orca also evaluates network misconfigurations and assigns risk accordingly. For example, developers often use external CI/CD services, such as Bitbucket, that require whitelisted IP address ranges. All customers using such an external CI/CD service are essentially exposing their internal services to the public internet. Orca will discover and alert on these risky configurations with a high risk score.



Orca Security

ASSET	SERVICE	ISSUE	RISK	ALERT
Server 1	Apache	CVE-2018-1176	Internet-facing PII Exposure	Imminent Compromise
Server 2	Apache	CVE-2018-1176	Internal Server	Hazardous
Server 3	SOL	-	-	None
Server 4	SOL	-	-	None

Server 1 and Server 2 have the same vulnerability. Server 1 is ranked higher, however, because it is easily accessible from the internet and is connected to a database containing PII.

ORCA COMBINES ASSET AND DATA CHARACTERISTICS WITH CONTEXT INFORMATION TO PRIORITIZE RISK AND ALERTS IN YOUR ENVIRONMENT

Reducing Analyst Fatigue

Getting a set of point security tools to talk to each other and provide clear correlated context about each finding is nearly impossible. Security personnel are left to establish context manually in order to understand and prioritize risk, leading to analyst fatigue.

Understanding risk context is critical and can turn a situation with poor security posture and analyst alert fatigue into strong security posture with energetic security personnel. Orca does the heavy lifting of contextualizing data and assessing the potential impact of vulnerabilities so analysts can focus on higher-value activities. Orca's mission is to provide the best contextualized security intelligence possible to improve security posture and reduce analyst fatigue.

For example, it's common for a machine that hasn't been patched in a while to have hundreds or even thousands of vulnerabilities. While other security tools might display an alert for each vulnerability, Orca is able to use context to reduce the number of alerts. For example, if an isolated machine has hundreds of vulnerabilities it will still receive a lower risk score from Orca because it's less vulnerable to attack. Orca's properly prioritized alerts and risk scores provide welcome relief for overworked security analysts.

Alert Automation and Integration

To further reduce alert fatigue and friction between teams, Orca allows security teams to query their cloud estate, and automate investigation and assignment of cloud security issues. Companies can leverage Orca's AI-powered search that allows users to ask natural language questions such as 'Do I have any log4j vulnerabilities that are public facing?' or "Do I have any unencrypted databases with sensitive data exposed to the Internet?"

Orca also allows teams to write their own custom alerts using Orca's intuitive query language. Queries can be run as oneoffs or as continuous alerts, and can be integrated with ticketing systems such as Jira, ServiceNow, and other Orca integration partners to enable highly efficient triage, remediation, notification, and compliance management.

Summary

Orca Security is leading cloud security innovation with the first platform to provide comprehensive public cloud security and compliance without the need for agents, combining the core capabilities of Cloud Security Posture Management, Cloud Workload Protection, Cloud Infrastructure Entitlement Management, API Security, Data Security Posture Management, AI Security, Vulnerability Management, and more—in a single platform. Orca is revolutionary, both in its approach to gathering cloud estate information and its ability to present risks and vulnerabilities in context.

Revolutionary SideScanning

Orca Security's patented SideScanning technology deploys in minutes and covers all cloud assets including virtual machines, cloud storage buckets, all types of containers and serverless functions in any mode of deployment, and much more. Orca Cloud Security Platform offers numerous benefits:

Agentless-first: Offering full coverage without agents, Orca leverages cloud configuration and workload data to build a fully contextualized asset inventory and perform a holistic security assessment of the entire cloud estate.

Single Platform: Orca's single platform eliminates the need to deploy multiple tools such as cloud vulnerability management, workload protection, API security, security posture management and compliance solutions.

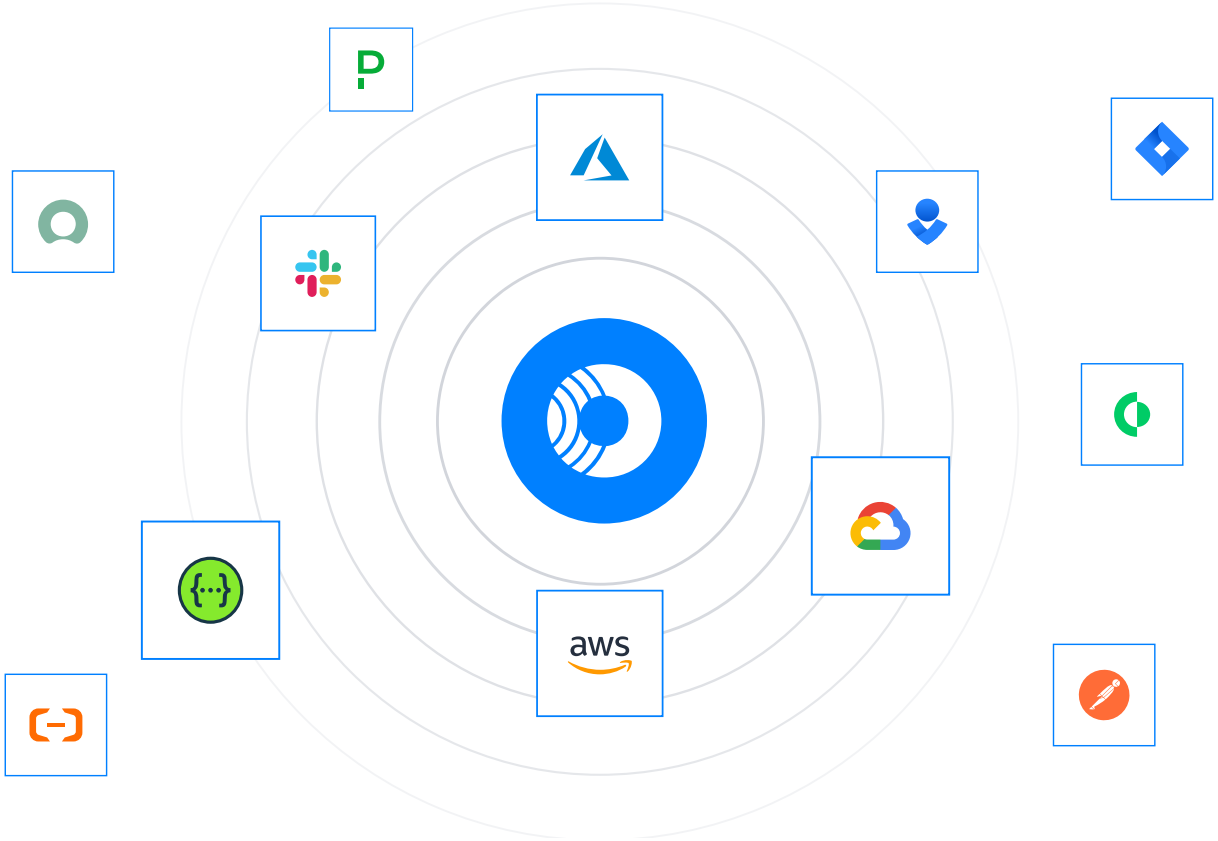
Risk Prioritization: Orca sees the big picture and prioritizes risks and attack paths based on environmental and business context. This reduces thousands of security alerts to the critical few that matter.

Deploy Once. Secure Forever: Because Orca Security is agentless-first, the platform deploys in minutes rather than weeks or months. With Orca Security, there are no gaps in coverage, no organizational friction, and no performance hits on cloud environments.

Orca significantly simplifies the efforts of cloud security teams to discover and remediate risk and vulnerabilities across complex multi-cloud environments. To achieve even further improvements in efficiency and TCO, organizations can customize alerts and automate ticketing to route issues directly to the proper teams for resolution.

Enterprise-Ready, Multi-Cloud Security

Orca is an enterprise-scalable platform designed to secure large multi-cloud estates efficiently and with low-overhead. With over 50 out-of-the-box third-party partner integrations, including Slack, OpsGenie, Jira, and ServiceNow, Orca helps maximize your organization's productivity. The platform also offers powerful alert query and automation capabilities that include auto-ticketing support and support for impactful workflows to speed up remediation, optimize collaboration, and minimize friction between your security, DevOps, and remediation teams.



About Orca Security

Orca Security is the industry-leading Cloud Security Platform that identifies, prioritizes, and remediates risks and compliance issues across your cloud estate spanning AWS, Azure, Google Cloud, Oracle Cloud, and Alibaba Cloud. Instead of layering multiple siloed tools together or requiring the need to deploy cumbersome agents, Orca delivers complete cloud security in a single platform by combining two revolutionary approaches: SideScanning, which enables frictionless and complete coverage without the need to maintain agents, and a Unified Data Model, which allows for centralized contextual analysis of your entire cloud estate.

Orca's agentless-first platform connects to your environment in minutes and provides comprehensive visibility of all your assets, automatically including new assets as they are added. Orca detects and prioritizes cloud risks across every layer of your cloud estate, including vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and overly permissive identities.

For more information or to schedule a demo, visit https://orca.security

TRUSTED BY ORGANIZATIONS ACROSS THE GLOBE

AUTODESK · Unity · GANNETT · Digital Turbine

POSTMAN · SAP · WILEY · Lemonade

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

COPYRIGHT 2024 ORCA SECURITY. ALL RIGHTS RESERVED

orca security