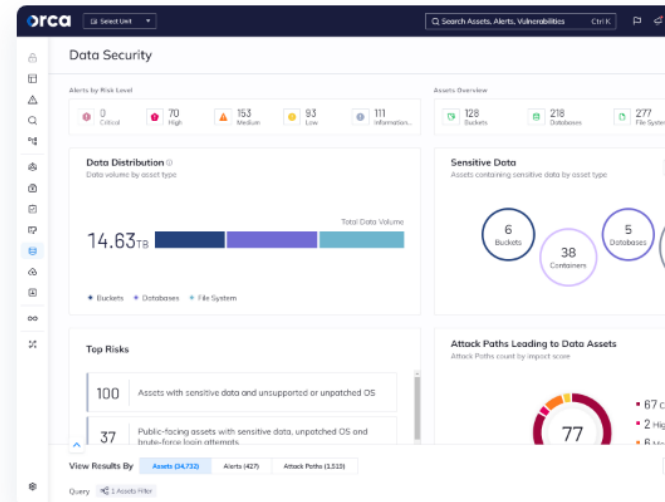


Sensitive Data Detection

Secure your most important data in the cloud with the Orca Cloud Security Platform. Orca scans your entire cloud estate to discover sensitive data at risk and prioritizes alerts based on environmental context.

[Get a Demo](#)


THE CHALLENGE

Legacy solutions create blind spots

Bad actors want your sensitive data, which is why protecting it is a top priority. But you can't protect what you can't see. Agent-based, legacy, or point solutions leave blindspots where sensitive data can hide that attackers can exploit.

- On average, less than 50% of assets are covered by agent-based solutions.
- Legacy tools, point solutions, and poorly integrated platforms don't fully contextualize risk, such as whether a data store is publicly exposed or connected to an internet-facing asset.



OUR APPROACH

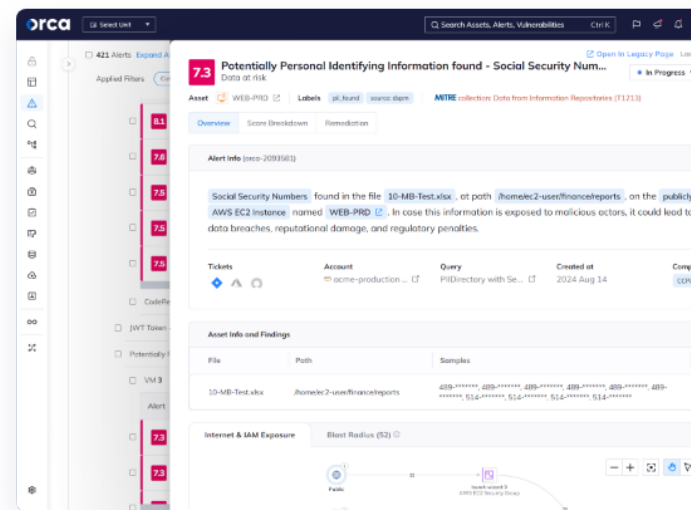
Protect your crown jewel assets with Orca's agentless data security tools

Orca detects sensitive data at-risk across both the workload and control plane, pinpointing the exact location and providing masked samples of the data for quick remediation. It also leverages context such as the location and accessibility of the assets containing the data. This approach separates the noise from the truly critical risks endangering your business.

Keep your sensitive data safe with complete coverage and risk detection

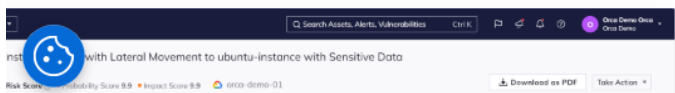
Orca scans the hidden corners of your cloud estate, searching for at-risk sensitive data, from personally identifiable information (PII) to protected healthcare information (PHI), and more.

- ✓ Detect at-risk sensitive data on every workload across your cloud estate, regardless of its state—whether running, idle, paused, or stopped.
- ✓ Alerts indicate the exact location of sensitive data and provide masked samples for efficient triaging and remediation.
- ✓ Sensitive data detection covers PII, including physical addresses, email addresses, credit card numbers, and Social Security identifiers.



How Orca classifies your crown jewels

Orca prioritizes threats and attack paths that endanger your most



How Orca classifies your crown jewels

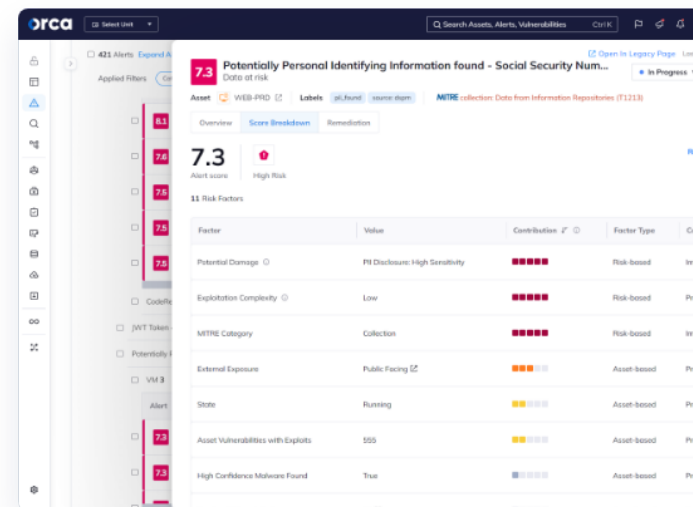
Orca prioritizes threats and attack paths that endanger your most critical assets, placing the focus on avoiding damaging data breaches and attacks, rather than giving all threats equal priority.

- ✓ To determine which assets are business critical, Orca automatically discovers sensitive data and critical assets, including assets with broad permission access and secrets exposure.
- ✓ Customers can also tag and classify critical assets themselves. Orca's "crown jewel" categories include Personal Identifiable Information (PII), intellectual property, financial information, and more.
- ✓ Any threats or attack paths that endanger the company's crown jewels, will automatically receive the highest priority and business impact score.

Orca cuts through the noise

Orca makes it easy to remediate at-risk sensitive data in the cloud. Statistical scanning and heuristics reduce the noise, while contextual analysis helps prioritize risk so security teams can focus on what truly matters.

- ✓ 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.
- ✓ Even with heuristic-based analysis, false positives are still possible. Orca provides the file location and several masked samples of potentially at-risk sensitive data to help you quickly identify false positives.
- ✓ When prioritizing alerts, Orca considers the accessibility of the surfaced sensitive data. For example, is the resource public facing? Is the workload stopped or paused? Does the asset that contains the sensitive data have critical vulnerabilities?



Complete visibility, minimal effort



Complete visibility, minimal effort

cake

LOCATION Europe

INDUSTRY Financial Services

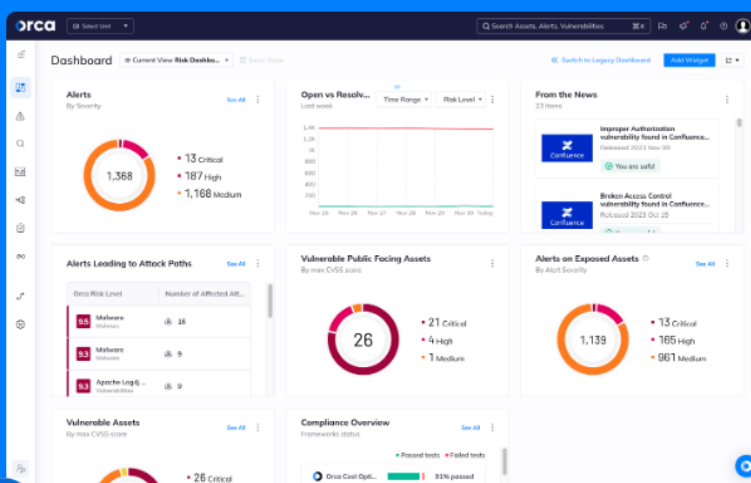
CLOUD ENVIRONMENT AWS

Read the Case Study

"We couldn't wait on periodic security checks. Orca helped us move to a method that's automated, that's checking every day, and that we can follow up on more easily."



Pieter Schelfhout
Head of Engineering



PERSONALIZED DEMO

See Orca Security in Action

Gain visibility, achieve compliance, and prioritize risks with the Orca Cloud Security Platform.

Get a Demo



Platform

CLOUD SECURITY PLATFORM

- Cloud Native Application Protection
- Vulnerability Management
- SideScanning™ Technology
- Container and Kubernetes Security
- Cloud Security Posture Management (CSPM)
- Cloud Infrastructure Entitlement Management (CIEM)
- Cloud Workload Protection Platform (CWPP)
- AI Security Posture Management (AI-SPM)
- Multi-Cloud Compliance and Security
- Cloud Detection and Response (CDR)
- Application Security
- API Security
- Data Security Posture Management (DSPM)
- Orca Sensor

TECHNOLOGY ECOSYSTEM

- Integrations
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- Oracle Cloud
- Alibaba Cloud

Solutions

BY SOLUTION

- Malware Detection
- Sensitive Data Detection
- IAM Risk
- Lateral Movement Risk

BY INDUSTRY

- Financial Services
- Technology
- Government
- Media & Entertainment
- Healthcare
- Retail

Resources

Library

- Product Info
- Podcast
- Case Studies
- Blog
- Events

COMPARISONS

- Prisma Cloud
- Qualys TotalCloud
- Lacework
- Rapid7
- Tenable
- Check Point

Company

- About
- Partners
- Reviews
- Orca Research Pod
- Careers
- Newsroom
- Media Kit

Contact

Support

Security Portal

User Center

Login

Stay in touch

Get cloud security insights and the latest Orca news

* Email Address

Submit

Awards & Certifications

- ✓ AWS Advanced Technology Partner Security Competency
- ✓ ISO/EC 27001 Information
- ✓ ISO/EC 27017 Information
- ✓ ISO/EC 27018 Information
- ✓ SOC 2 TYPE II Certified
- ✓ 2022 AWS Global Security Partner of the Year
- ✓ Star Level One: Self-Assessment Cloud Security Alliance
- ✓ CSA Trusted Cloud Provider Cloud Security Alliance

