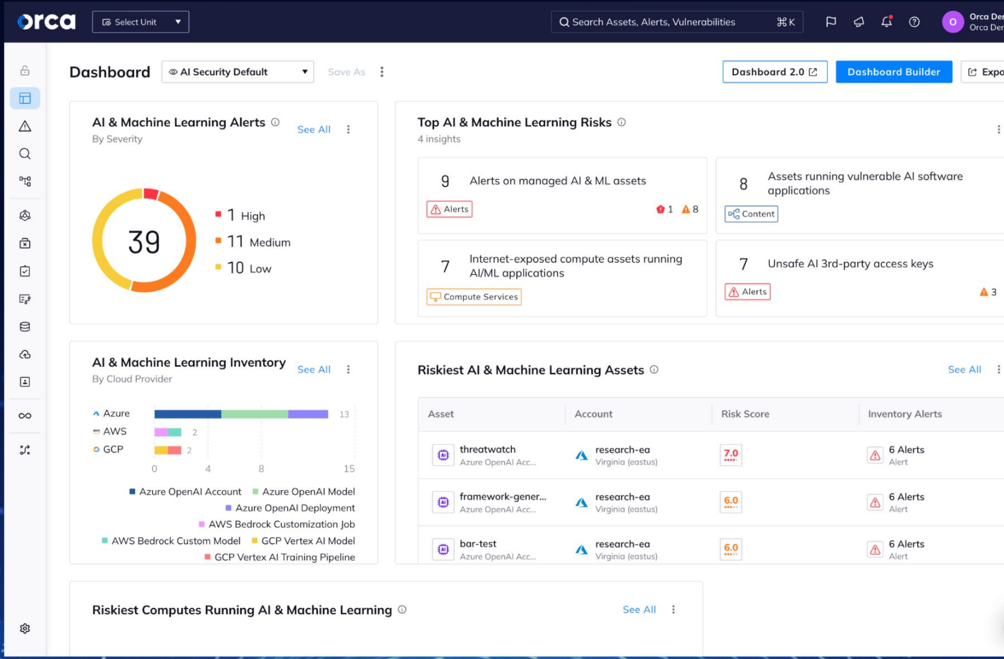
Orca Cloud Security Platform Overview


orca
Select Unit
Search Assets, Alerts, Vulnerabilities ⌘K
Orca Dem
Orca Dem
Dashboard
AI Security Default
Save As
Dashboard 2.0
Dashboard Builder
Expo
AI & Machine Learning Alerts
By Severity
See All
39
1 High
11 Medium
10 Low
Top AI & Machine Learning Risks
4 insights
9 Alerts on managed AI & ML assets
Alerts
1
8
8 Assets running vulnerable AI software applications
Content
7 Internet-exposed compute assets running AI/ML applications
Compute Services
7 Unsafe AI 3rd-party access keys
Alerts
3
AI & Machine Learning Inventory
By Cloud Provider
See All
Azure
AWS
GCP
13
2
2
0
4
8
15
Azure OpenAI Account
Azure OpenAI Model
Azure OpenAI Deployment
AWS Bedrock Customization Job
AWS Bedrock Custom Model
GCP Vertex AI Model
GCP Vertex AI Training Pipeline
Riskiest AI & Machine Learning Assets
See All
Riskiest Computes Running AI & Machine Learning
See All

Asset	Account	Risk Score	Inventory Alerts
threatwatch Azure OpenAI Acc...	research-ea Virginia (eastus)	7.0	6 Alerts Alert
framework-gener... Azure OpenAI Acc...	research-ea Virginia (eastus)	6.0	6 Alerts Alert
bar-test Azure OpenAI Acc...	research-ea Virginia (eastus)	6.0	6 Alerts Alert

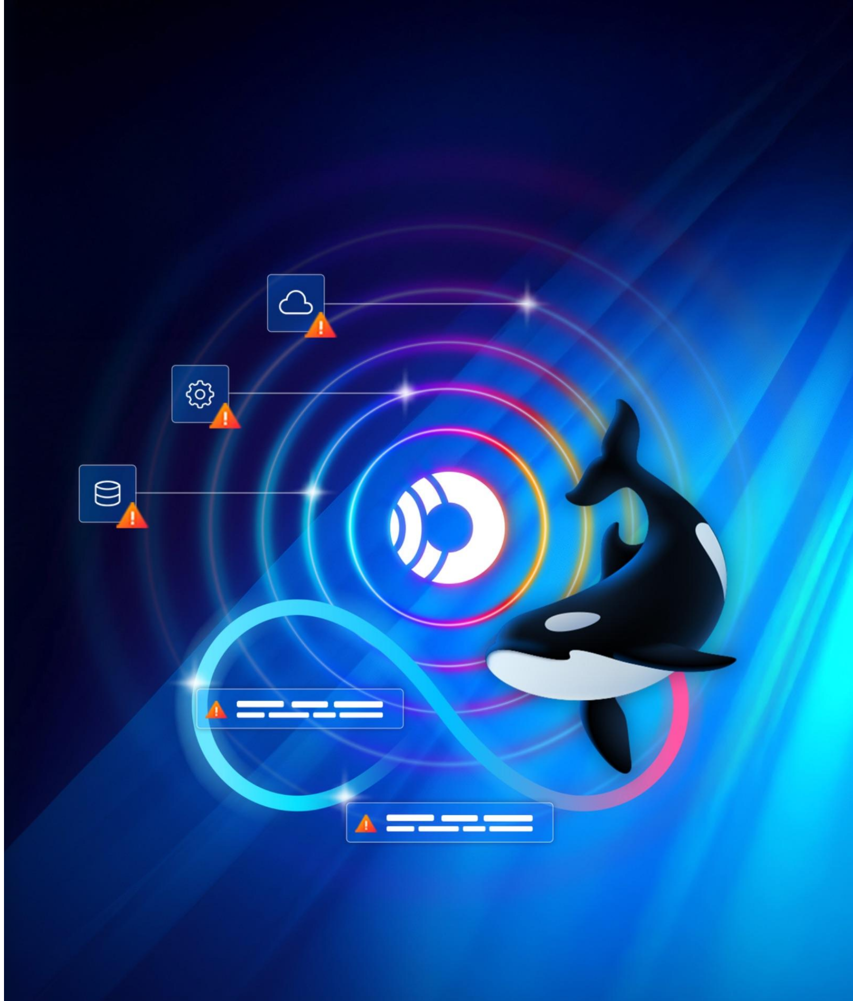
Table of Contents

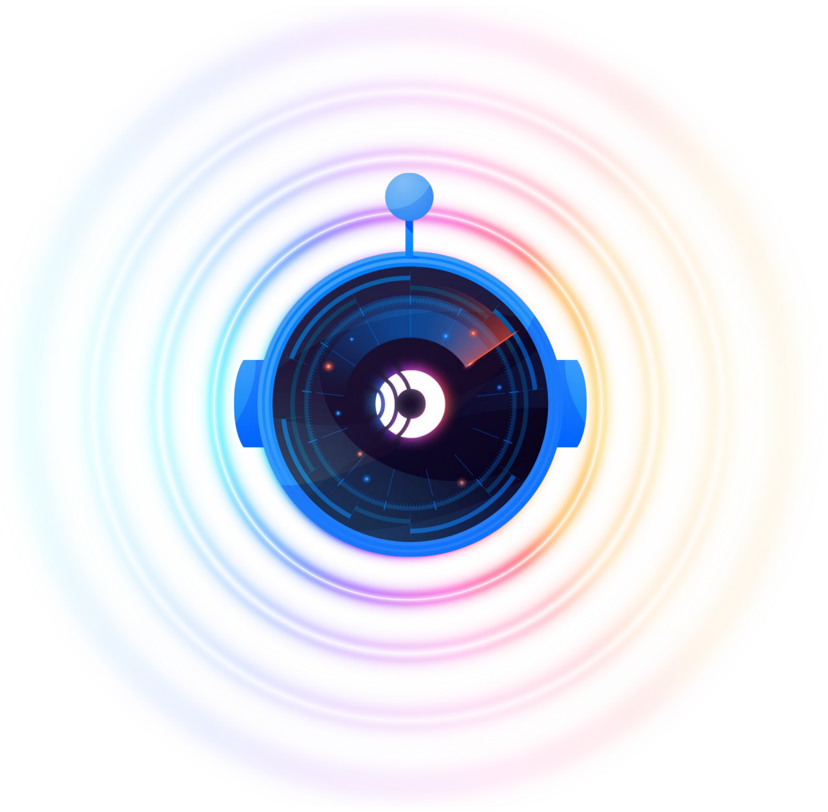
ORCA CLOUD SECURITY PLATFORM

Orca is Delivering the Platform of the Future

Orca identifies, prioritizes, and remediates risks and compliance issues in workloads, configurations, and identities across your cloud estate spanning AWS, Azure, Google Cloud, Kubernetes, Alibaba Cloud, and Oracle Cloud. Orca offers the industry's most comprehensive cloud security solution in a single platform —eliminating the need to deploy and maintain multiple point solutions.

The Orca Cloud Security Platform unifies security across your organization, combining critical pre-deployment capabilities (AppSec) with runtime security (CNAPP) that offers a fully integrated, lightweight sensor.





ORCA CLOUD SECURITY PLATFORM

Integrated Runtime Security for Advanced CDR

Orca provides advanced Cloud Detection and Response (CDR) that combines the power of agentless CDR with fully integrated, lightweight runtime protection for your sensitive workloads.

With Orca, you can leverage prioritized alerts that cover all CDR use cases, fully contextualize forensic findings, and streamline remediation.

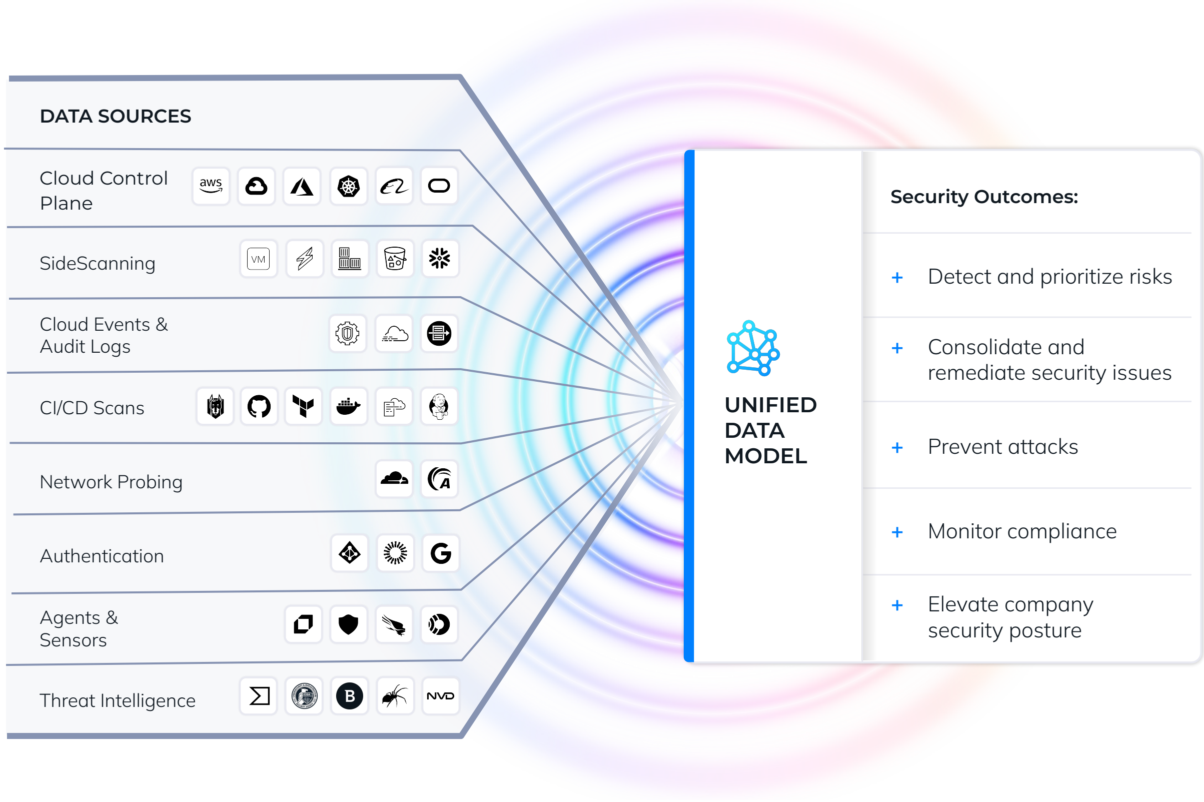
The Orca Platform also integrates with your entire security stack, ingesting cloud logs from AWS GuardDuty, Azure Defender for Cloud, GCP Security Command Center, while also supporting deep integrations with SIEM, SOAR, and other security tools.

ORCA CLOUD SECURITY PLATFORM

Unified Data Model

Orca's Unified Data Model contextualizes all your data sources to unify the intelligence collected from cloud workloads, configurations, identities, and much more.

This powerful approach enables Orca to build a graph-based map of your cloud estate, giving you complete visibility into your cloud assets and their relationships. The map surfaces truly critical security issues and their root causes, enabling you to make measurable improvements to your cloud security posture while avoiding alert fatigue.



DATA SOURCES

- Cloud Control Plane
- SideScanning
- Cloud Events & Audit Logs
- CI/CD Scans
- Network Probing
- Authentication
- Agents & Sensors
- Threat Intelligence

UNIFIED DATA MODEL

Security Outcomes:

+ Detect and prioritize risks
+ Consolidate and remediate security issues
+ Prevent attacks
+ Monitor compliance
+ Elevate company security posture

Lemonade

> *“Orca is without a doubt the most important cloud security product we’ve got. It’s hard to overstate the importance of having a digestible source of information that doesn’t overwhelm you or inspire loathing.”*

JONATHAN JAFFE,

CHIEF INFORMATION SECURITY OFFICER

Orca Cloud Security Platform

Key Capabilities

CORE CLOUD SECURITY

- Cloud Security Posture Management (CSPM)
- Multi-Cloud Compliance
- Kubernetes Security Posture Management (KSPM)
- Cloud Workload Protection Platform (CWPP)
- Vulnerability Management
- Cloud Infrastructure Entitlement Management (CIEM)

ADVANCED SECURITY

- Cloud Detection and Response (CDR)
- Application Security (AppSec)
- API Security
- Data Security (DSPM)
- AI-Security (AI-SPM)

PLATFORM FEATURES

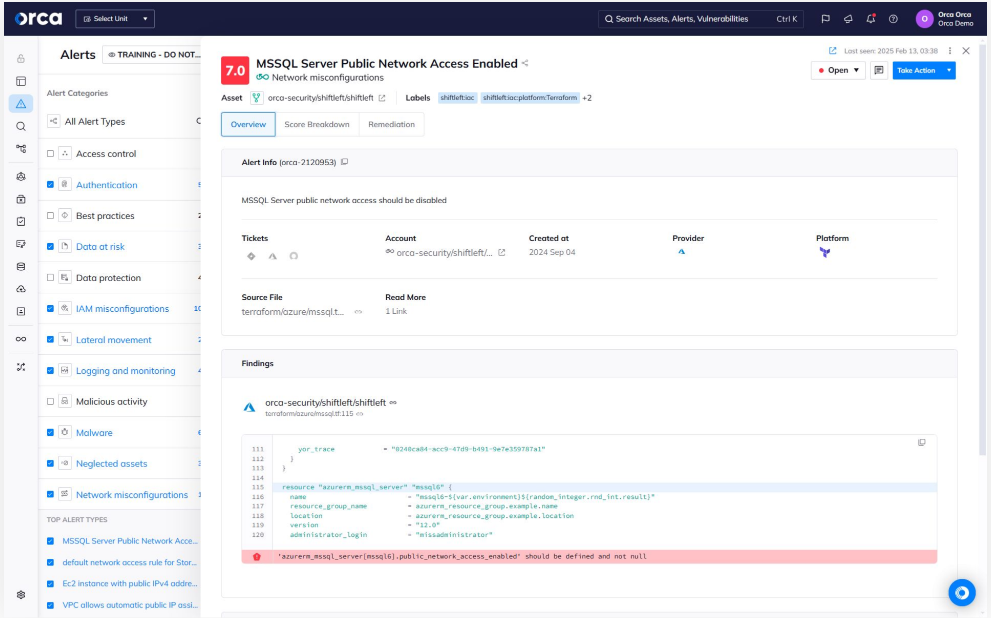
- Role-Based Access Control (RBAC)
- Single Sign-On (SSO)
- Business Unit Support
- Integrations (such as Jira, ServiceNow, Slack)
- Reporting
- Scheduled Reports
- Early Access to Beta Features

TECHNICAL SUPPORT

- Standard Support Level
- Support Service Upgrade (Elite)3

DEPLOYMENT MODE

- SAAS
- In-account or Private



7.0 MSSQL Server Public Network Access Enabled

Network misconfigurations

Asset orca-security/shiftleft/shiftleft

Labels shiftleft:iac shiftleft:iac:platform:Terraform +2

Alert Info (orca-2120953)

MSSQL Server public network access should be disabled

Tickets

Account: orca-security/shiftleft/...

Created at: 2024 Sep 04

Provider

Platform

Source File: terraform/azure/mssql.t...

Read More: 1 Link

Findings

orca-security/shiftleft/shiftleft

terraform/azure/mssql.tf:115

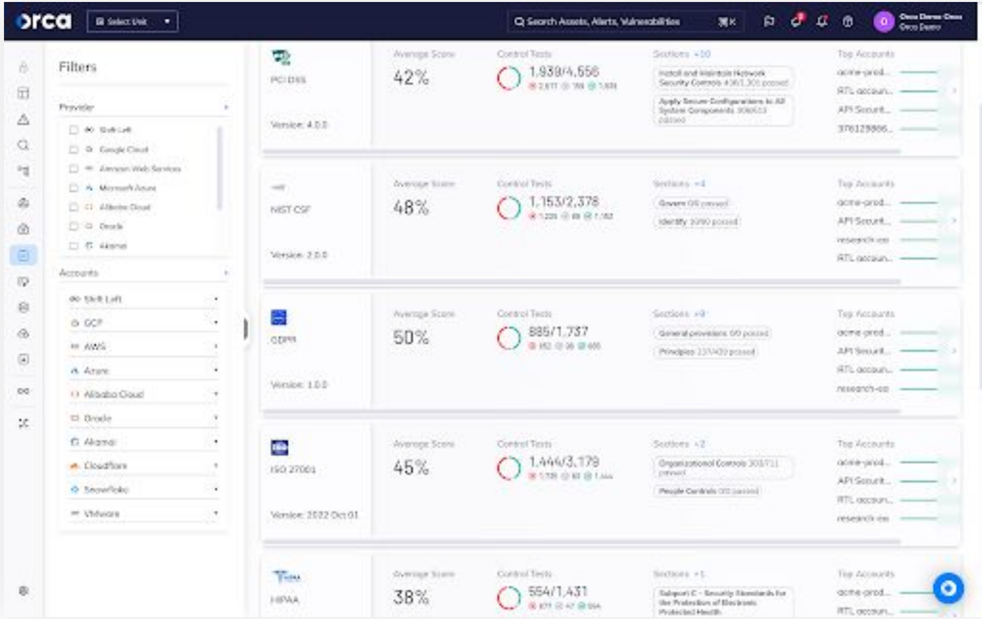
```
    yor_trace           = "0240ca84-acc9-47d9-b491-9e7e359787a1"
  }
}

resource "azurerm_mssql_server" "mssql6" {
  name                         = "mssql6-${var.environment}${random_integer.rnd_int.result}"
  resource_group_name          = azurerm_resource_group.example.name
  location                     = azurerm_resource_group.example.location
  version                      = "12.0"
  administrator_login          = "missadministrator"
'azurerm_mssql_server[mssql6].public_network_access_enabled' should be defined and not null
```

Cloud Security Posture Management (CSPM)

Orca's Cloud Security Posture Management (CSPM) solution continuously checks for misconfigurations, ensures multi-cloud compliance, and goes beyond traditional solutions to combine CSPM with CWPP, CIEM, CDR, DSPM, and more from one unified platform.

Orca's CSPM capabilities leverage 2,500+ configuration controls across 10+ categories and automatically checks configurations & policies against 185+ compliance frameworks.



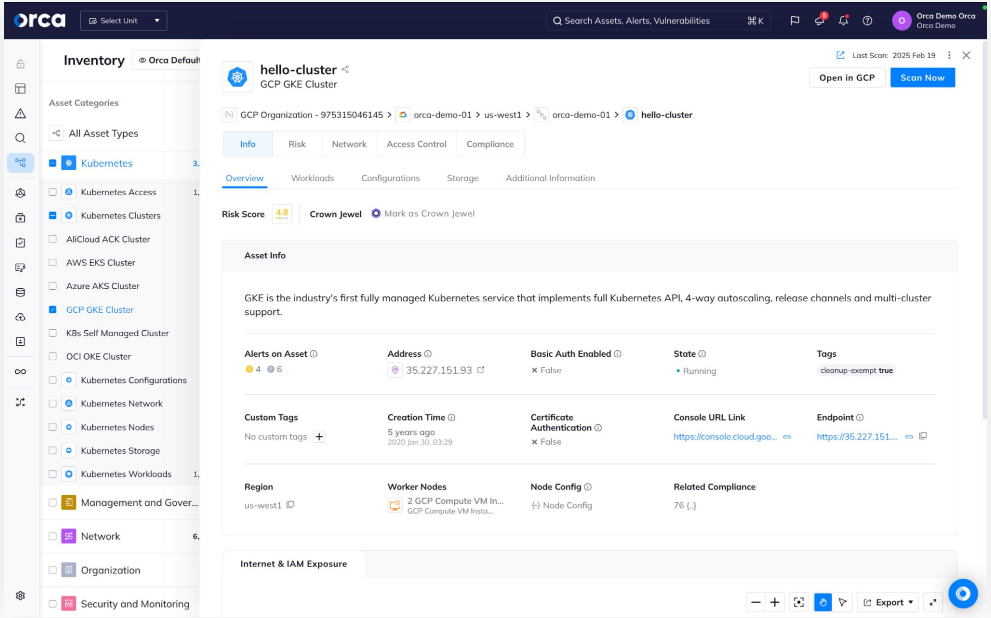
Framework	Average Score	Control Tests	Sections	Top Accounts
PCI DSS Version: 4.0.0	42%	1,939/4,556	Sections +10 Install and Maintain Network Security Controls Apply Secure Configurations to All System Components	acme-prod... RTL accoun... API Securit... 376123886...
NIST CSF Version: 2.0.0	48%	1,153/2,378	Sections +4 Govern Identify	acme-prod... API Securit... research-... RTL accoun...
GDPR Version: 1.0.0	50%	885/1,737	Sections +9 General provisions Principles	acme-prod... API Securit... RTL accoun... research-...
ISO 27001 Version: 2022 Oct 01	45%	1,444/3,179	Sections +2 Organizational Controls People Controls	acme-prod... API Securit... RTL accoun... research-...
HIPAA	38%	554/1,431	Sections +1 Subpart C - Security Standards for the Protection of Electronic Protected Health	acme-prod... RTL accoun...

2

Multi-Cloud Compliance

Orca's Multi-Cloud Compliance capabilities accelerate and automate your compliance efforts across AWS, Azure, Google Cloud, Oracle Cloud, and Alibaba Cloud.

Orca offers 185+ built-in and customizable compliance frameworks and CIS benchmarks, fast and flexible options for remediation, and customizable and automated exporting/reporting options.



hello-cluster
GCP GKE Cluster

GCP Organization - 975315046145 > orca-demo-01 > us-west1 > orca-demo-01 > **hello-cluster**

Risk Score 4.8 | Crown Jewel ○ Mark as Crown Jewel

Asset Info

GKE is the industry's first fully managed Kubernetes service that implements full Kubernetes API, 4-way autoscaling, release channels and multi-cluster support.

Alerts on Asset
4 6

Address
35.227.151.93

Basic Auth Enabled
× False

State
● Running

Tags
cleanup-exempt **true**

Custom Tags
No custom tags +

Creation Time
5 years ago
2020 Jan 30, 03:29

Certificate Authentication
× False

Console URL Link
https://console.cloud.goo...

Endpoint
https://35.227.151....

Region
us-west1

Worker Nodes
2 GCP Compute VM In...
GCP Compute VM Insta...

Node Config
{··} Node Config

Related Compliance
76 {..}

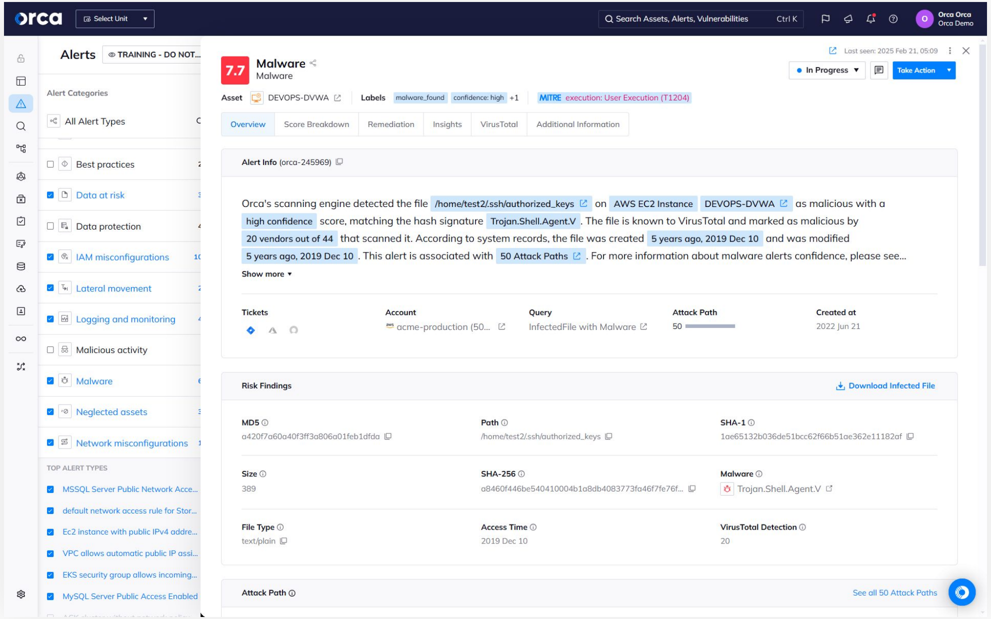
Internet & IAM Exposure

3

Kubernetes Security Posture Management (KSPM)

The Orca Platform offers Kubernetes Security Posture Management (KSPM) capabilities that provide full visibility into and across clusters.

The feature detects and prioritizes risks, and offers continuous compliance checks for CIS benchmarks, cloud service providers, STIG, and OWASP Kubernetes Top 10.



- ☐ Best practices
- ☑ Data at risk
- ☐ Data protection
- ☑ IAM misconfigurations
- ☑ Lateral movement
- ☑ Logging and monitoring
- ☐ Malicious activity
- ☑ Malware
- ☑ Neglected assets
- ☑ Network misconfigurations

TOP ALERT TYPES

- ☑ MSSQL Server Public Network Acce...
- ☑ default network access rule for Stor...
- ☑ Ec2 instance with public IPv4 addre...
- ☑ VPC allows automatic public IP assi...
- ☑ EKS security group allows incoming...
- ☑ MySQL Server Public Access Enabled

7.7 **Malware**
Malware

Asset DEVOPS-DVWA **Labels** malware_found confidence: high +1 MITRE execution: User Execution (T1204)

Alert Info (orca-245969)

Orca's scanning engine detected the file /home/test2/.ssh/authorized_keys on AWS EC2 Instance DEVOPS-DVWA as malicious with a high confidence score, matching the hash signature Trojan.Shell.Agent.V . The file is known to VirusTotal and marked as malicious by 20 vendors out of 44 that scanned it. According to system records, the file was created 5 years ago, 2019 Dec 10 and was modified 5 years ago, 2019 Dec 10 . This alert is associated with 50 Attack Paths . For more information about malware alerts confidence, please see...

Tickets	Account	Query	Attack Path	Created at
	acme-production (50...	InfectedFile with Malware	50	2022 Jun 21

Risk Findings

MD5 a420f7a60a40f3ff3a806a01feb1dfda	**Path** /home/test2/.ssh/authorized_keys	**SHA-1** 1ae65132b036de51bcc62f66b51ae362e11182af
Size 389	**SHA-256** a8460f446be540410004b1a8db4083773fa46f7fe76f...	**Malware** Trojan.Shell.Agent.V
File Type text/plain	**Access Time** 2019 Dec 10	**VirusTotal Detection** 20

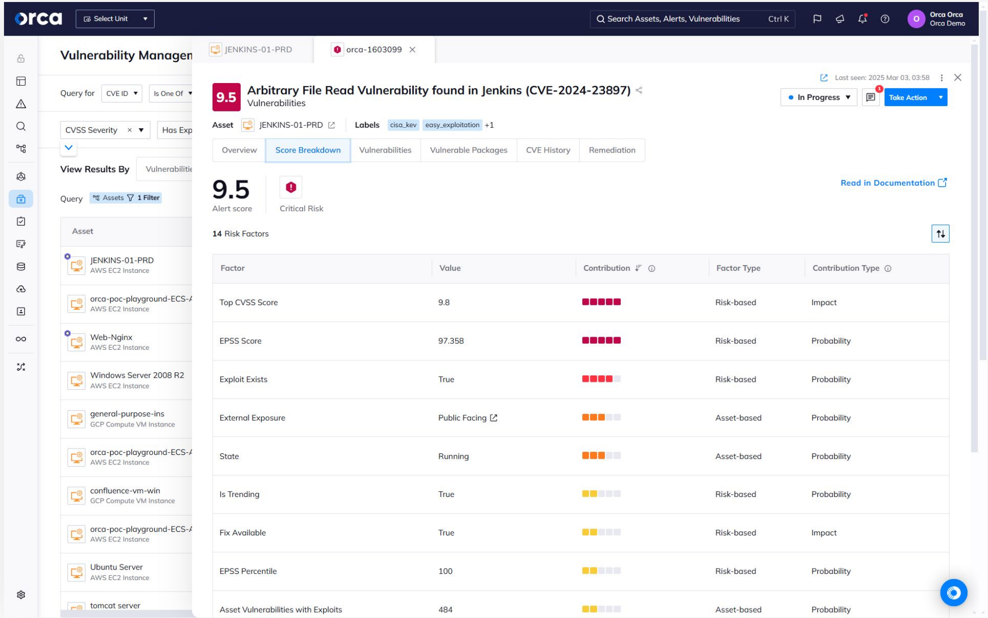
Attack Path

4

Cloud Workload Protection Platform (CWPP)

Orca's Cloud Workload Protection Platform (CWPP) solution provides full visibility into your cloud workloads, covering VMs, containers, Kubernetes clusters, and serverless functions.

The solution identities, prioritizes, and remediates your critical risks, including known and unknown malware.



Vulnerability Managen

Query for CVE ID Is One Of

CVSS Severity × Has Exp

View Results By Vulnerabilitie

Query Assets 1 Filter

Asset
JENKINS-01-PRD AWS EC2 Instance
orca-poc-playground-ECS-A AWS EC2 Instance
Web-Nginx AWS EC2 Instance
Windows Server 2008 R2 AWS EC2 Instance
general-purpose-ins GCP Compute VM Instance
orca-poc-playground-ECS-A AWS EC2 Instance
confluence-vm-win GCP Compute VM Instance
orca-poc-playground-ECS-A AWS EC2 Instance
Ubuntu Server AWS EC2 Instance
tomcat server

9.5 Arbitrary File Read Vulnerability found in Jenkins (CVE-2024-23897)
Vulnerabilities

Last seen: 2025 Mar 03, 03:58

In Progress | Take Action

Asset JENKINS-01-PRD | Labels cisa_kev easy_exploitation +1

Overview | Score Breakdown | Vulnerabilities | Vulnerable Packages | CVE History | Remediation

9.5
Alert score

Critical Risk

Read in Documentation

14 Risk Factors

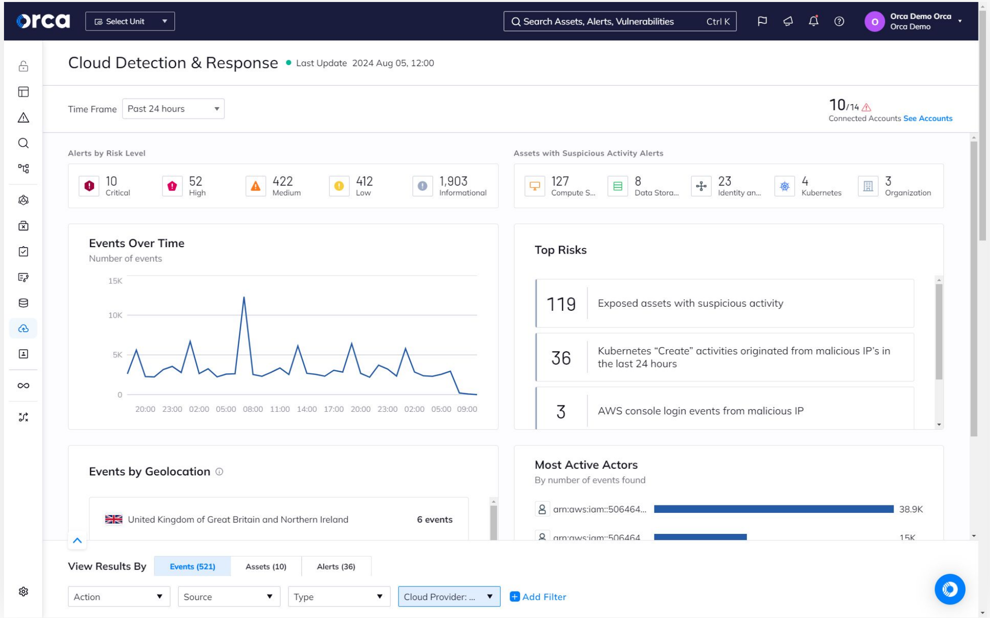
Factor	Value	Contribution	Factor Type	Contribution Type
Top CVSS Score	9.8	■■■■■	Risk-based	Impact
EPSS Score	97.358	■■■■■	Risk-based	Probability
Exploit Exists	True	■■■■□	Risk-based	Probability
External Exposure	Public Facing	■■■□□	Asset-based	Probability
State	Running	■■■□□	Asset-based	Probability
Is Trending	True	■■□□□	Risk-based	Probability
Fix Available	True	■■□□□	Risk-based	Impact
EPSS Percentile	100	■■□□□	Risk-based	Probability
Asset Vulnerabilities with Exploits	484	■■□□□	Asset-based	Probability

5

Vulnerability Management

Orca’s Vulnerability Management capabilities leverage 20+ vulnerability data sources to discover and prioritize vulnerabilities across your entire cloud estate.

The solution goes beyond CVSS scores to analyze and prioritize vulnerabilities holistically using a comprehensive set of risk- and asset-based factors. It also enables you to streamline remediation with AI-driven and assisted options.



Cloud Detection & Response ● Last Update 2024 Aug 05, 12:00

Time Frame: Past 24 hours

10/14 Connected Accounts See Accounts

Alerts by Risk Level

10	52	422	412	1,903
Critical	High	Medium	Low	Informational

Assets with Suspicious Activity Alerts

127	8	23	4	3
Compute S...	Data Stora...	Identity an...	Kubernetes	Organization

Events Over Time

Number of events

Top Risks

119	Exposed assets with suspicious activity
36	Kubernetes “Create” activities originated from malicious IP’s in the last 24 hours
3	AWS console login events from malicious IP

Events by Geolocation

United Kingdom of Great Britain and Northern Ireland — 6 events

Most Active Actors

By number of events found

arn:aws:iam::506464...	38.9K
arn:aws:iam::506464	15K

View Results By: Events (521) | Assets (10) | Alerts (36)

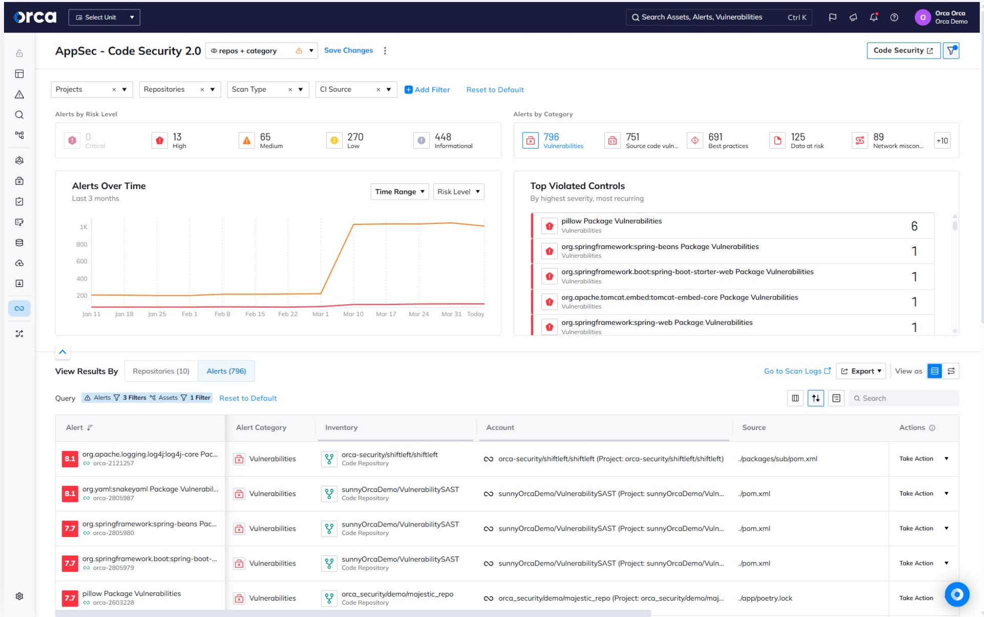
6

Cloud Detection and Response (CDR)

Orca’s Cloud Detection and Response (CDR) capabilities combine the power of agentless CDR with fully integrated, lightweight runtime security.

Orca combines 24×7 monitoring of cloud provider logs and threat intelligence feeds with insights into existing risks to identify and prioritize potentially dangerous events that require immediate attention.

Orca also provides real-time visibility, detection, investigation, and prevention for your critical workloads.



AppSec - Code Security 2.0

Alerts by Risk Level

0	13	65	270	448
Critical	High	Medium	Low	Informational

Alerts by Category

796	751	691	125	89	+10
Vulnerabilities	Source code vuln...	Best practices	Data at risk	Network miscon...	

Alerts Over Time

Last 3 months

Top Violated Controls

By highest severity, most recurring

pillow Package Vulnerabilities Vulnerabilities	6
org.springframework:spring-beans Package Vulnerabilities Vulnerabilities	1
org.springframework.boot:spring-boot-starter-web Package Vulnerabilities Vulnerabilities	1
org.apache.tomcat.embed:tomcat-embed-core Package Vulnerabilities Vulnerabilities	1
org.springframework:spring-web Package Vulnerabilities Vulnerabilities	1

View Results By

Query: Alerts 3 Filters Assets 1 Filter

Alert	Alert Category	Inventory	Account	Source	Actions
8.1 org.apache.logging.log4j:log4j-core Pac... orca-2121257	Vulnerabilities	orca-security/shiftleft/shiftleft Code Repository	orca-security/shiftleft/shiftleft (Project: orca-security/shiftleft/shiftleft)	./packages/sub/pom.xml	Take Action
8.1 org.yaml:snakeyaml Package Vulnerabil... orca-2805987	Vulnerabilities	sunnyOrcaDemo/VulnerabilitySAST Code Repository	sunnyOrcaDemo/VulnerabilitySAST (Project: sunnyOrcaDemo/Vuln...	./pom.xml	Take Action
7.7 org.springframework:spring-beans Pac... orca-2805980	Vulnerabilities	sunnyOrcaDemo/VulnerabilitySAST Code Repository	sunnyOrcaDemo/VulnerabilitySAST (Project: sunnyOrcaDemo/Vuln...	./pom.xml	Take Action
7.7 org.springframework.boot:spring-boot-... orca-2805979	Vulnerabilities	sunnyOrcaDemo/VulnerabilitySAST Code Repository	sunnyOrcaDemo/VulnerabilitySAST (Project: sunnyOrcaDemo/Vuln...	./pom.xml	Take Action
7.7 pillow Package Vulnerabilities orca-2603228	Vulnerabilities	orca_security/demo/majestic_repo Code Repository	orca_security/demo/majestic_repo (Project: orca_security/demo/maj...	./app/poetry.lock	Take Action

7

Application Security (AppSec)

Orca delivers critical Application Security (AppSec) capabilities to secure your applications as you design and build them.

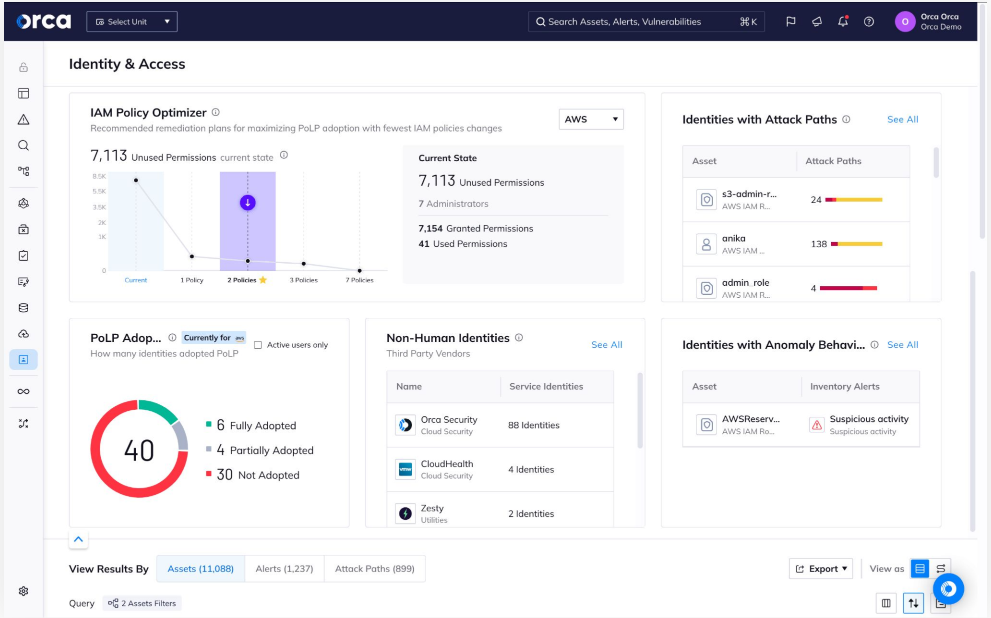
This includes comprehensive guardrail policies to catch issues before production and Cloud-to-Dev capabilities that trace cloud risks to their code origins and remediate issues at their source.

Orca also enhances the developer experience with two-way integrations with SCM and ticketing systems, ensuring that they can access security findings in their preferred tools and workflows.

8 Cloud Infrastructure Entitlement Management (CIEM)

Orca's Cloud Infrastructure Entitlement Management (CIEM) solution gives you full visibility into all identities, roles, groups, permissions, and policies deployed in your cloud environment.

The solution prioritizes alerts for identity and entitlement risks, supports multi-cloud compliance, and optimizes IAM policies to enforce the principle of least privilege (PoLP).



Identity & Access

IAM Policy Optimizer

Recommended remediation plans for maximizing PoLP adoption with fewest IAM policies changes

7,113 Unused Permissions current state

Current State

7,113 Unused Permissions

7 Administrators

7,154 Granted Permissions

41 Used Permissions

Identities with Attack Paths

Asset	Attack Paths
s3-admin-r... AWS IAM R...	24
anika AWS IAM ...	138
admin_role AWS IAM R...	4

PoLP Adop...

Currently for aws

☐ Active users only

How many identities adopted PoLP

- 6 Fully Adopted
- 4 Partially Adopted
- 30 Not Adopted

Non-Human Identities

Third Party Vendors

Name	Service Identities
Orca Security Cloud Security	88 Identities
CloudHealth Cloud Security	4 Identities
Zesty Utilities	2 Identities

Identities with Anomaly Behavi...

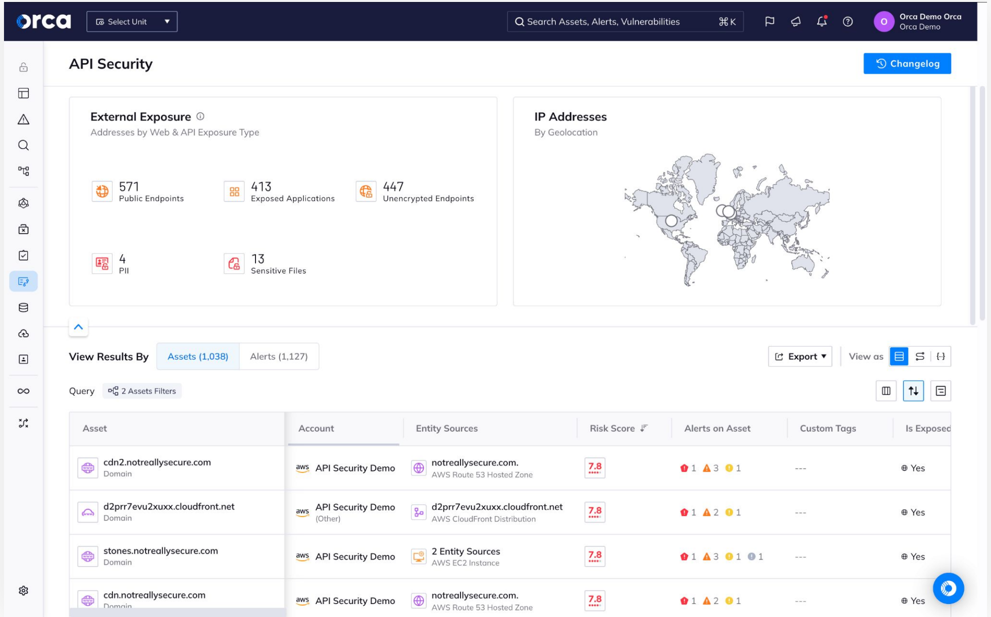
Asset	Inventory Alerts
AWSReserv... AWS IAM Ro...	Suspicious activity Suspicious activity

View Results By: Assets (11,088) | Alerts (1,237) | Attack Paths (899)

Query: 2 Assets Filters

9

API Security



API Security

External Exposure
Addresses by Web & API Exposure Type

571	Public Endpoints
413	Exposed Applications
447	Unencrypted Endpoints
4	PII
13	Sensitive Files

IP Addresses
By Geolocation

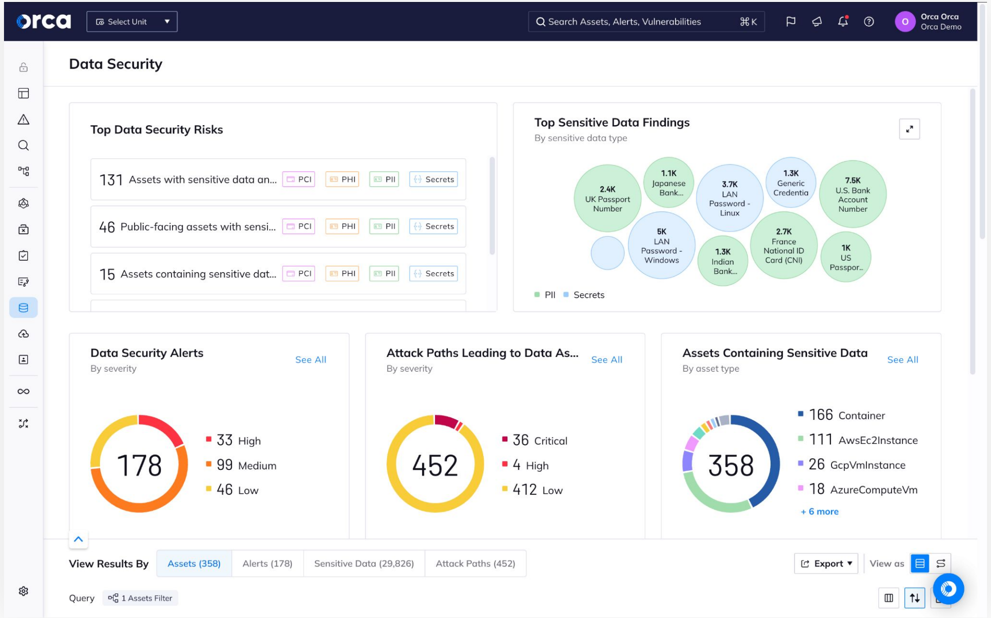
View Results By: Assets (1,038) | Alerts (1,127)

Query: 2 Assets Filters

Asset	Account	Entity Sources	Risk Score	Alerts on Asset	Custom Tags	Is Exposed
cdn2.notreallysecure.com Domain	aws API Security Demo	notreallysecure.com. AWS Route 53 Hosted Zone	7.8	1 3 1	---	Yes
d2prr7evu2xuxx.cloudfront.net Domain	aws API Security Demo (Other)	d2prr7evu2xuxx.cloudfront.net AWS CloudFront Distribution	7.8	1 2 1	---	Yes
stones.notreallysecure.com Domain	aws API Security Demo	2 Entity Sources AWS EC2 Instance	7.8	1 3 1 1	---	Yes
cdn.notreallysecure.com Domain	aws API Security Demo	notreallysecure.com. AWS Route 53 Hosted Zone	7.8	1 2 1	---	Yes

Orca’s API Security capabilities continuously discover and inventory managed and unmanaged API assets, including applications, domains, subdomains, path groups, users, and API endpoints.

The feature enables you to understand exposure and prioritize detection and remediation with context-based insights. Orca also continuously monitors API behavior and usage and alerts teams to potentially unwanted drift.

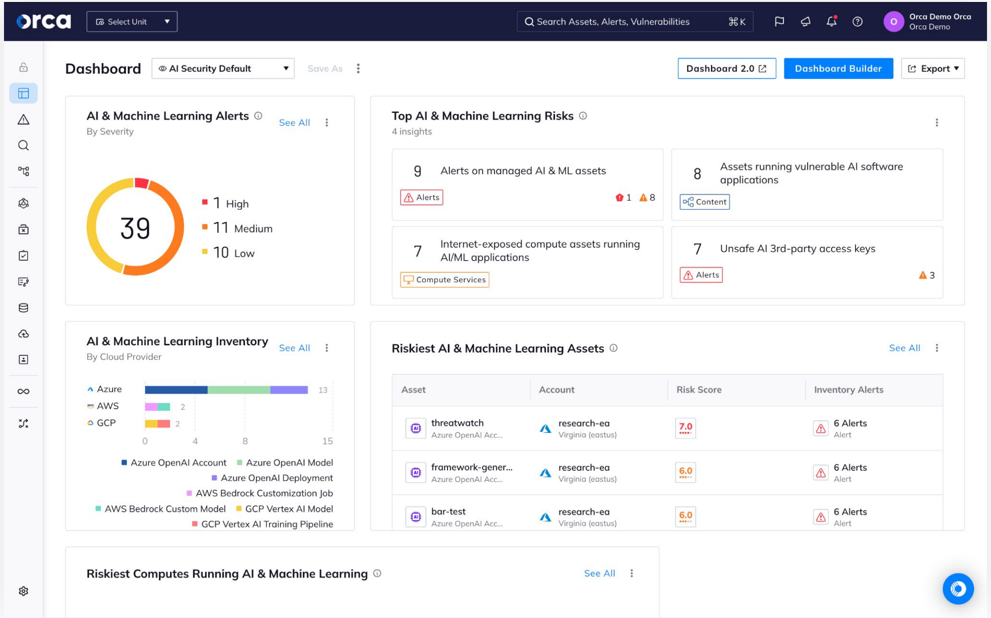


10

Data Security (DSPM)

Orca's Data Security (DSPM) capabilities enable you to discover and classify data in your cloud, including PII, PCI, PHI, financial information, SSH Keys, and more. I

t enables you to ensure continuous compliance with data privacy mandates and regulations, as well as detect suspicious activity and understand dangerous attack paths to reduce risk.



AI & Machine Learning Alerts
By Severity

Top AI & Machine Learning Risks
4 insights

9 Alerts on managed AI & ML assets — Alerts — 1 — 8

8 Assets running vulnerable AI software applications — Content

7 Internet-exposed compute assets running AI/ML applications — Compute Services

7 Unsafe AI 3rd-party access keys — Alerts — 3

AI & Machine Learning Inventory
By Cloud Provider

Riskiest AI & Machine Learning Assets

Asset	Account	Risk Score	Inventory Alerts
threatwatch Azure OpenAI Acc...	research-ea Virginia (eastus)	7.0	6 Alerts Alert
framework-gener... Azure OpenAI Acc...	research-ea Virginia (eastus)	6.0	6 Alerts Alert
bar-test Azure OpenAI Acc...	research-ea Virginia (eastus)	6.0	6 Alerts Alert

Riskiest Computes Running AI & Machine Learning

11

AI Security (AI-SPM)

Orca's AI Security (AI-SPM) capabilities enable you to secure your AI cloud assets.

The feature identities 50+ AI models and software packages, discovers sensitive data stored in AI projects, and prioritizes and remediates AI risks.

sisense

> *“Orca Security is unique in that it locates vulnerabilities with precision and delivers tangible, actionable results —without having to sift through all of the noise.”*

AARON BROWN,

SENIOR CLOUD SECURITY ENGINEER

SAP	unity	7 ELEVEN	AUTODESK
WILEY	Raiffeisen Bank	paidy	vivino
GRUBHUB	RSA	Digital Turbine	Lemonade
druva	G|H GRAHAM HOLDINGS	Solarisbank	Vercel
catawiki	C6 BANK	HUNTERS	CHEQ
OU	GANNETT	Carlsberg	sisense
nrg	signifyhealth	job&talent	MAILINBLACK

About Orca Security

Orca enables organizations to make cloud security a strategic advantage. With the most comprehensive coverage and visibility across multi-cloud environments, the agentless-first Orca Platform unites teams to eliminate complexities, vulnerabilities and risks.

Backed by Temasek, CapitalG, ICONIQ Capital, Redpoint Ventures and others, Orca is trusted by hundreds of organizations, including SAP, Gannett, Autodesk, Unity, Lemonade and Digital Turbine.

↗ To find out more, schedule a personalized demo of the Orca platform.

orca SECURITY