



# Comprehensive Cloud Security – In Minutes

The Industry-Leading Agentless  
Cloud Security Platform

# Orca Security at-a-Glance



**Founded in 2019,**  
with innovative, patent-pending  
approach to cloud security



**Veteran Executive Team**  
Check Point, Palo Alto Networks,  
Fastly, Twistlock, and Unit 8200



**\$630M funding /  
\$1.8B valuation**



**350+ employees**

## Executive Team



Avi Shua  
CEO



Pini Karuchi  
CFO and COO



Gil Geron  
CPO



Yoav Alon  
CTO



Meghan Marks  
CMO



Terry Hill  
CRO

## Investors



## Awards



# The Research Pod: Discovering the cloud's emerging risks



**Dedicated** researchers finding emerging cloud native threats



**Major** cloud native CVEs disclosed, including AutoWarp, BreakingFormation, Superglue, and SynLapse



**1200+** risks publicly detailed in the Cloud Risk Encyclopedia

The screenshot shows the Orca Security Cloud Risk Encyclopedia website. The header includes the Orca Security logo and navigation links for Platform, Solutions, Partners, About, Resources, and Research. There are buttons for 'Test Drive' and 'Watch Demo'. The main heading is 'Cloud Risk Encyclopedia' with a subtext: 'Search 1200+ cloud security risks or filter by cloud vendor, compliance framework, risk category, and criticality. 3 cloud platforms. 29 compliance frameworks. 18 risk categories. 4 risk levels.' Below this is a search bar with the placeholder text 'Search over 1200 cloud risks from Orca's platform...'. A 'Featured Cloud Risks' section displays three items: 'Superglue: A remediated zero-day vulnerability in AWS Glue', 'BreakingFormation: Vulnerability in AWS CloudFormation', and 'Cross-Account Access Without External ID or MFA'. Each item has a lock icon and the label 'REMIEDIATED VULNERABILITY'.

**The Register**

Orca Security Tells AWS Fail Tail with Happy Ending

**VentureBeat**

Major Microsoft Cross-Tenant Vulnerability Caught by Orca Security

**The Hacker News**

Microsoft Mitigates RCE Vulnerability Impacting Synapse & Data Factory



# Trusted by **hundreds** of leading enterprises across the globe



WILEY



SAP



Rapyd



LIONBRIDGE

eMed.

GANNETT



Lemonade



Metromile



Wix



# Our Principles:

## Four Cs for Cloud Security Success



### Coverage

Cloud security requires 100% visibility and coverage of the entire cloud estate.



### Comprehensive

The cloud must be secured holistically  
– one solution to detect all security risks.



### Context

Cloud security findings are best understood as attack vectors, rather than siloed alerts.



### Consumable

It's all about taking loads of data and making it consumable and actionable so that teams can use it to support decision making.

# Challenges



## Problem #1: Agents Don't Scale

Less than **50%** of cloud assets are covered by host security solutions

Difficult to deploy everywhere

Significant performance degradation

Causes organization friction

Very high Total Cost of Ownership (TCO)



## Problem #2: Alert Overload

For every **100** assets there are an average **10,000** alerts

Multiple tools working in silos

Prioritization is difficult

Alert fatigue



What is Orca?

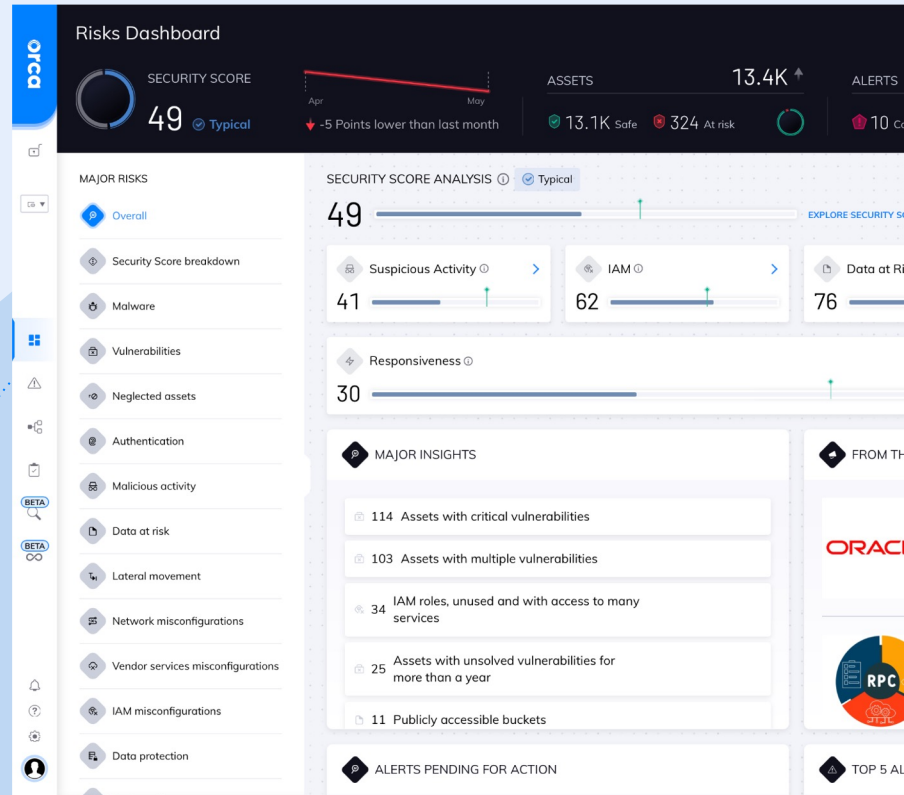
# Complete Coverage Across Cloud Risks

**Agentless scanning** provides complete coverage of all cloud assets

**Identify, address and prioritize** all cloud risks

**Automatically surface attack paths** to find the vital risks that matter

**Implement CI/CD controls** to embed security early in the development process





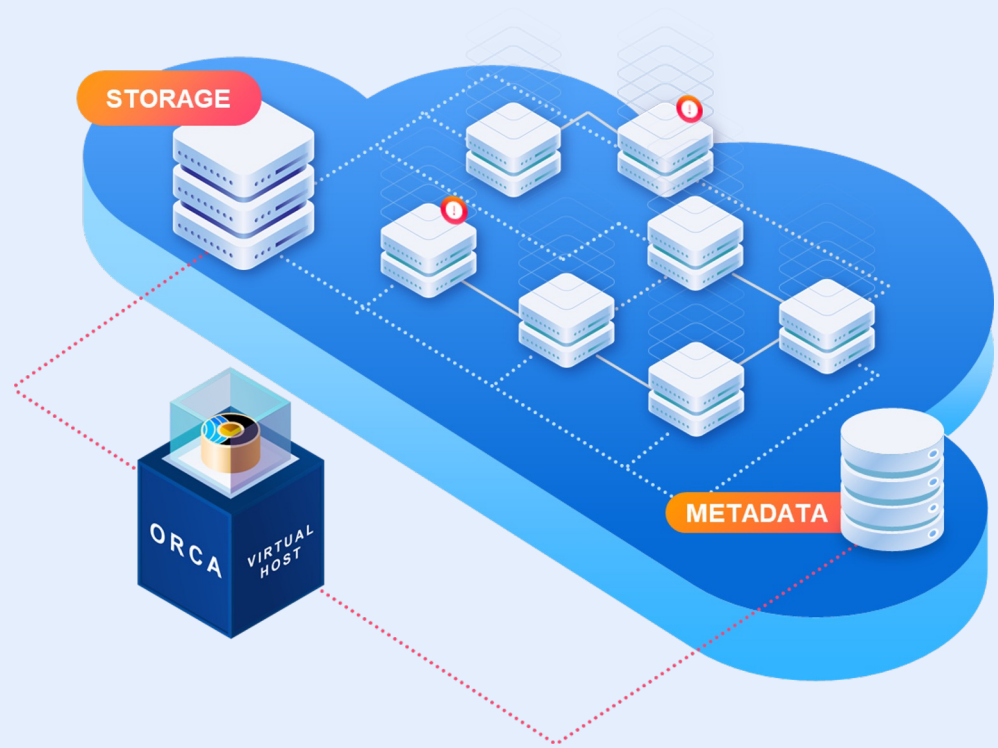
# Orca is Powered by our Patent Pending SideScanning™

Eliminate the need for Agents  
and Sidecars

Collect data directly from

- Each workload's runtime block storage
- Cloud APIs

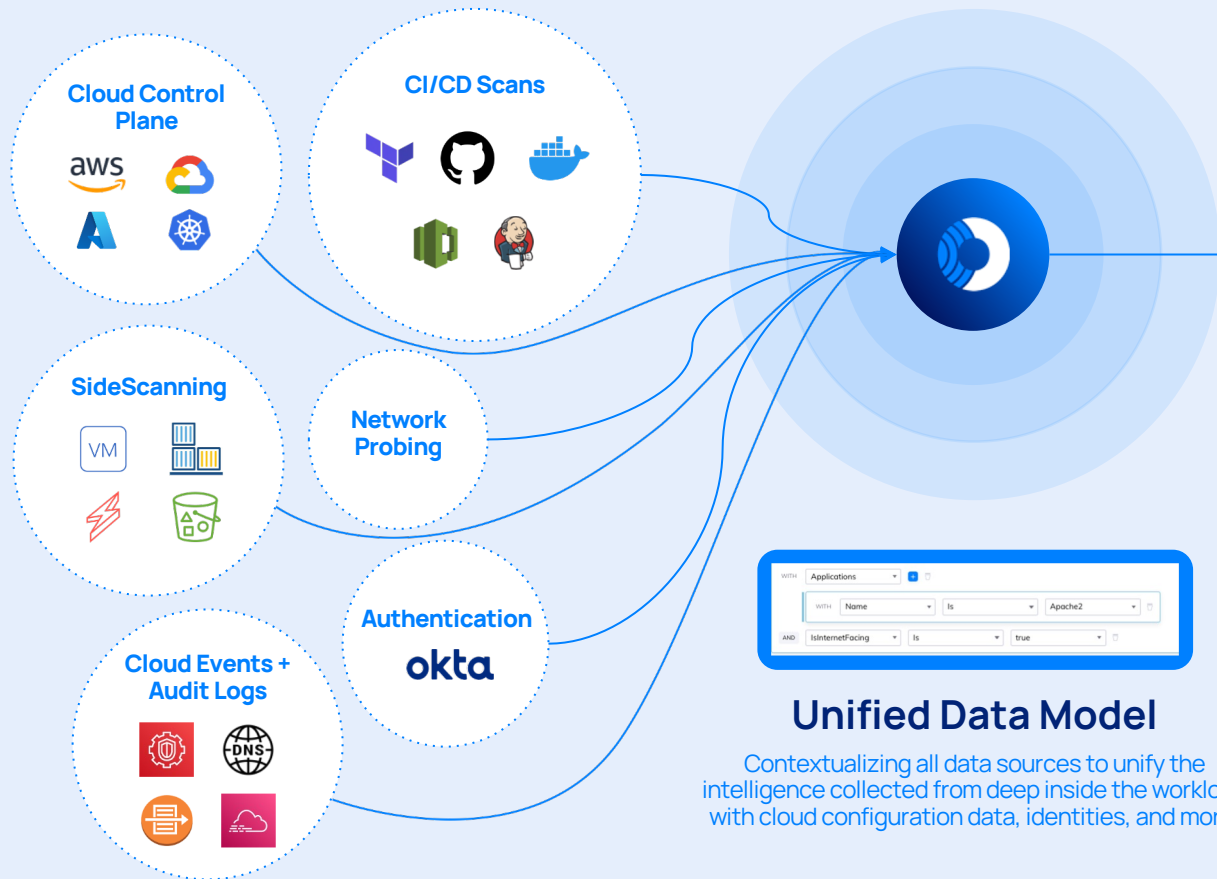
Gain immediate context to understand  
risks and their importance across your  
entire cloud estate







## Data Sources



## Security Outcomes

- Asset Inventory
- Prioritized Alerts
- IAM Risks
- Cloud Compliance
- Remediation & Orchestration Integrations
- Cloud Detection & Response
- Isolation & Control



# Identify & Address All Cloud Risks

## Risks

## Orca Capabilities

 Vulnerabilities	.....	Coverage of OS, applications, and libraries
 Misconfigurations	.....	Prioritization across cloud infrastructure and workloads
 Data Exposure	.....	Alert on insecure data and PII
 Authentication & Entitlements	.....	Identify over-permissioned accounts and identity risks
 Malware	.....	Signature- and heuristic-based detection
 API & Web Application Exposure	.....	Inventory of managed and unmanaged APIs
 Lateral Movement Risks	.....	Alert on insecure keys and improper segmentation

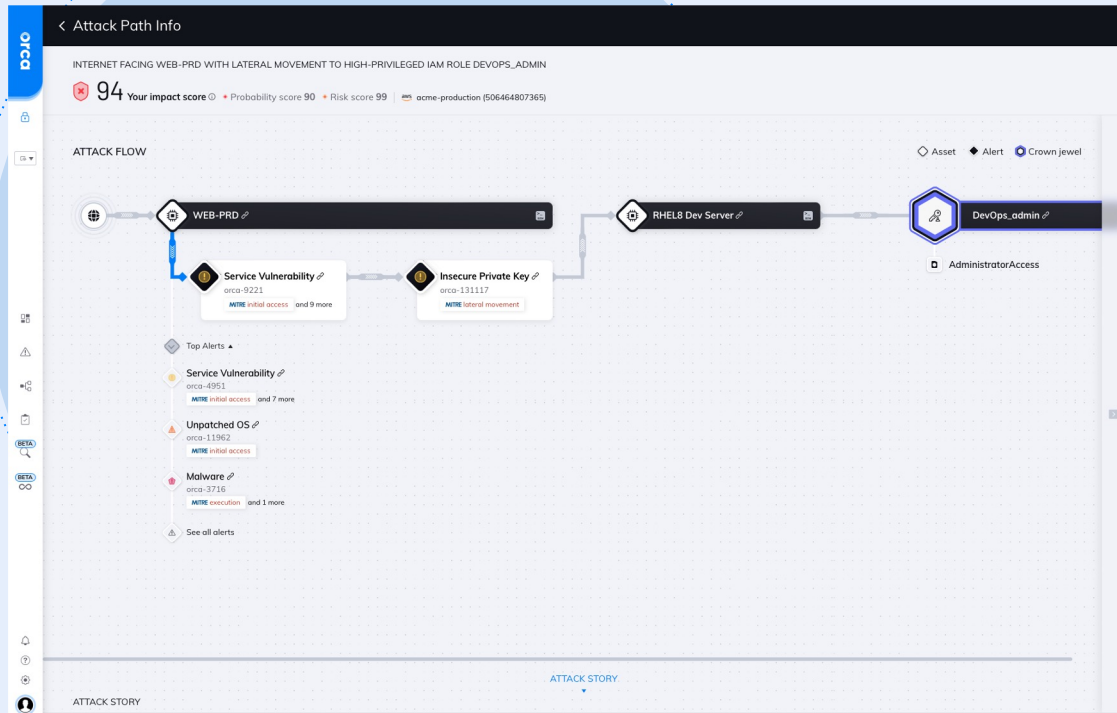


# Automatically Surface Attack Paths To Focus on Risks that Matter

Deeply understand toxic combinations of security issues

Easily understand top risks with scoring and identification of crown jewel risks

MITRE ATT&CK mappings and detailed Attack Story ensure you and your teams understand the risk





# Integrated CI/CD Controls To Shift Security Left

Identify vulnerabilities and misconfigurations across the pipeline

Enforce policies to prevent insecure deployments in container images and IaC templates

Natively integrated to cloud native technologies and DevOps tools:



Single scan result

postgres:14.2

SCAN DETAILS

SCAN FAILED SUMMARY CONTROLS INSIGHTS VULNERABILITY INSIGHTS

CLI Version 1.0.3 Image ID sha256:95700231f9c263702... Runtime 05-12-2022 14:38 1 Failed 5 Warn 12 Passed 2 Critical 20 High 7 Medium 87 Low

Project Default Project Image Digest sha256:ab0be6280ada8549f... Ran by Joey\_test\_GPC

ATTACHED POLICIES

Orca Built-in - Container Image Best Practices Policy Failed

1 of 14 controls failed

Status	Title	Priority
Failed	Container image should be created with a non-root user	HIGH

See all

Orca Built-in - Vulnerabilities Policy Passed

Vulnerabilities

Status	CVE name	Target	Type	Severity	CvssScore3	CvssScore2	Package Name	Package Version	Fixed Version	Published Date
Warning	CVE-2022-1292	OS Packages	debian	Critical	9.8	10	libssl1.1	1.1.1n-0+deb11u1		03.05.2022
Warning	CVE-2022-1292	OS Packages	debian	Critical	9.8	10	openssl	1.1.1n-0+deb11u1		03.05.2022
Warning	CVE-2022-1271	OS Packages	debian	High	7.1		gzip	1.10-4	1.10-4+deb11u1	
Warning	CVE-2022-1271	OS Packages	debian	High	7.1		libzmq5	5.2.5-2	5.2.5-2.1+deb11u1	
Passed	CVE-2022-1304	OS Packages	debian	High	7.8	6.8	e2fsprogs	1.46.2-2		14.04.2022
Passed	CVE-2021-3999	OS Packages	debian	High	7.4		libc-bin	2.31-13+deb11u3		



Life with Orca

# Orca Security: The Cloud is Yours

- Easy 1-2-3 one-time deployment
- Scans your entire cloud estate in minutes
- Act on critical issues immediately
- Shifts security left – as part of development and DevOps workflows
- Covers 100% of your assets -- now and in the future

The screenshot displays the 'Attack Path Info' interface in Orca Security. At the top, it shows the title '< Attack Path Info' and a summary: 'INTERNET FACING ASSET WITH LATERAL MOVEMENT TO DEV-RND'. Below this, a score of '85' is shown with a red shield icon, accompanied by 'Your path score', 'Probability score 81', and 'Risk score 90'. The main section is titled 'ATTACK FLOW' and features a flow diagram. The flow starts with a globe icon, moves to a 'Web-Nginx' node, then to a 'Service Vulnerability' node (orca-9218) with a yellow warning icon, and finally to an 'Insecure Private Key' node (orca-108919) with a red warning icon. Below the flow diagram, there is a 'Top Alerts' section with three entries, each for a 'Service Vulnerability' (orca-5329, orca-4733, and orca-2988), each with a yellow warning icon and a 'MITRE initial access' tag. A 'See all alerts' link is at the bottom of this section. The interface includes a sidebar on the left with various navigation icons and a 'BETA' badge.

# Thank you!

