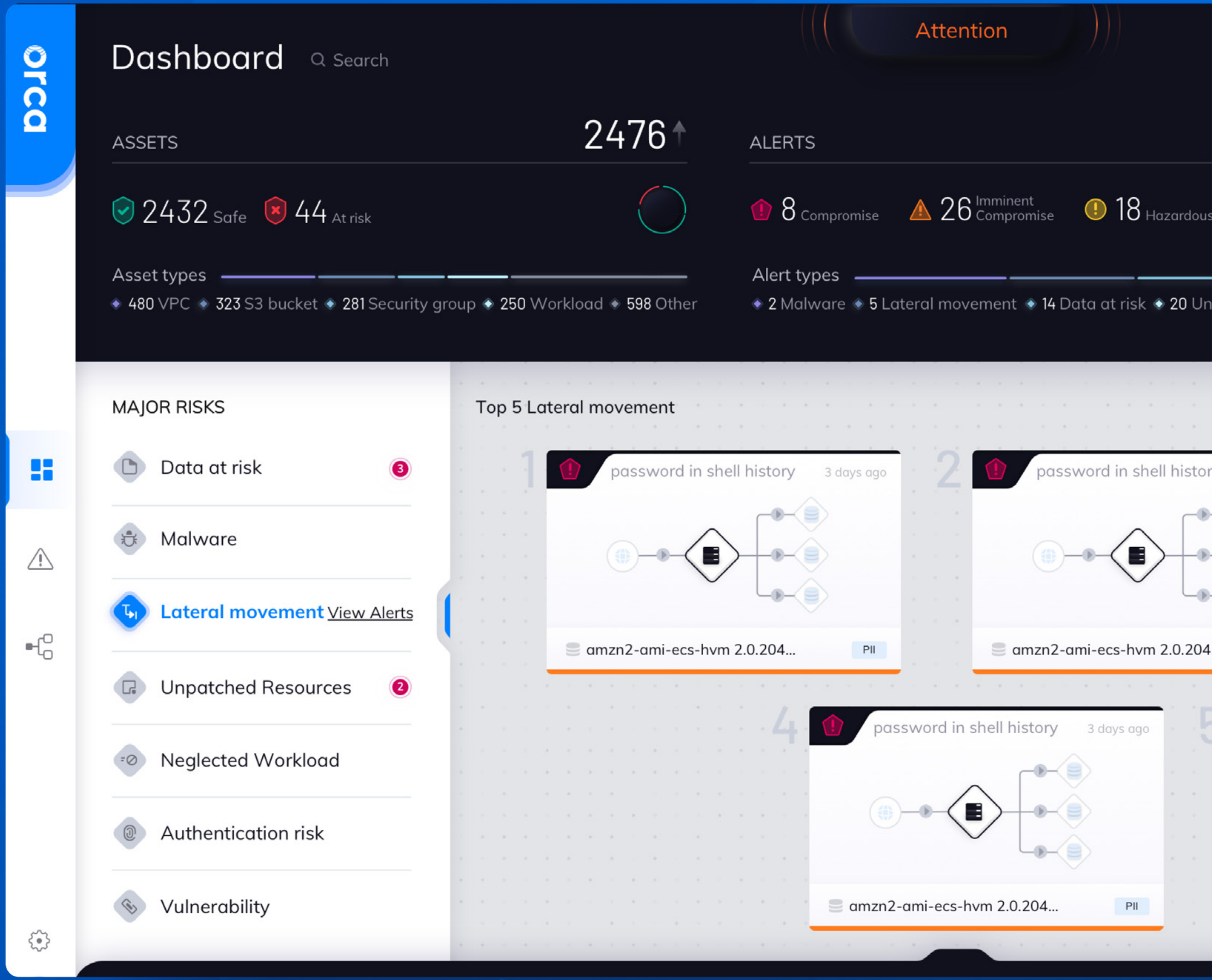
ORCA AGENTLESS CLOUD SECURITY PLATFORM

Cloud Security That Actually Works



Dashboard Search

Attention

ASSETS 2476

2432 Safe 44 At risk

Asset types

480 VPC · 323 S3 bucket · 281 Security group · 250 Workload · 598 Other

ALERTS

8 Compromise 26 Imminent Compromise 18 Hazardous

Alert types

2 Malware · 5 Lateral movement · 14 Data at risk · 20 Un

MAJOR RISKS

Data at risk	3
Malware	
Lateral movement View Alerts	
Unpatched Resources	2
Neglected Workload	
Authentication risk	
Vulnerability	

Top 5 Lateral movement

1 password in shell history 3 days ago
amzn2-ami-ecs-hvm 2.0.204... PII

2 password in shell histor
amzn2-ami-ecs-hvm 2.0.204

4 password in shell history 3 days ago
amzn2-ami-ecs-hvm 2.0.204... PII

Companies in nearly every industry have embraced the cloud. But while cloud adoption has matured, cloud security has been slow to catch up, and it's putting mission critical workloads at risk. Companies can't afford to slow down their innovation in the cloud, nor can they continue to operate with outdated tools. It's time security and DevOps teams have the capabilities they need to work seamlessly, efficiently, and securely in the cloud.

> Enterprise adoption of cloud-native applications quadrupled over a three-year period.
>
> THE EVEREST GROUP

Last-generation security tools were not designed for the cloud. They were built for the legacy, slow changing on-premises world of yesterday. These tools rely on outdated deployment methods like agents and utilize operational models that are at complete odds with the core principles of cloud computing: agility and speed.

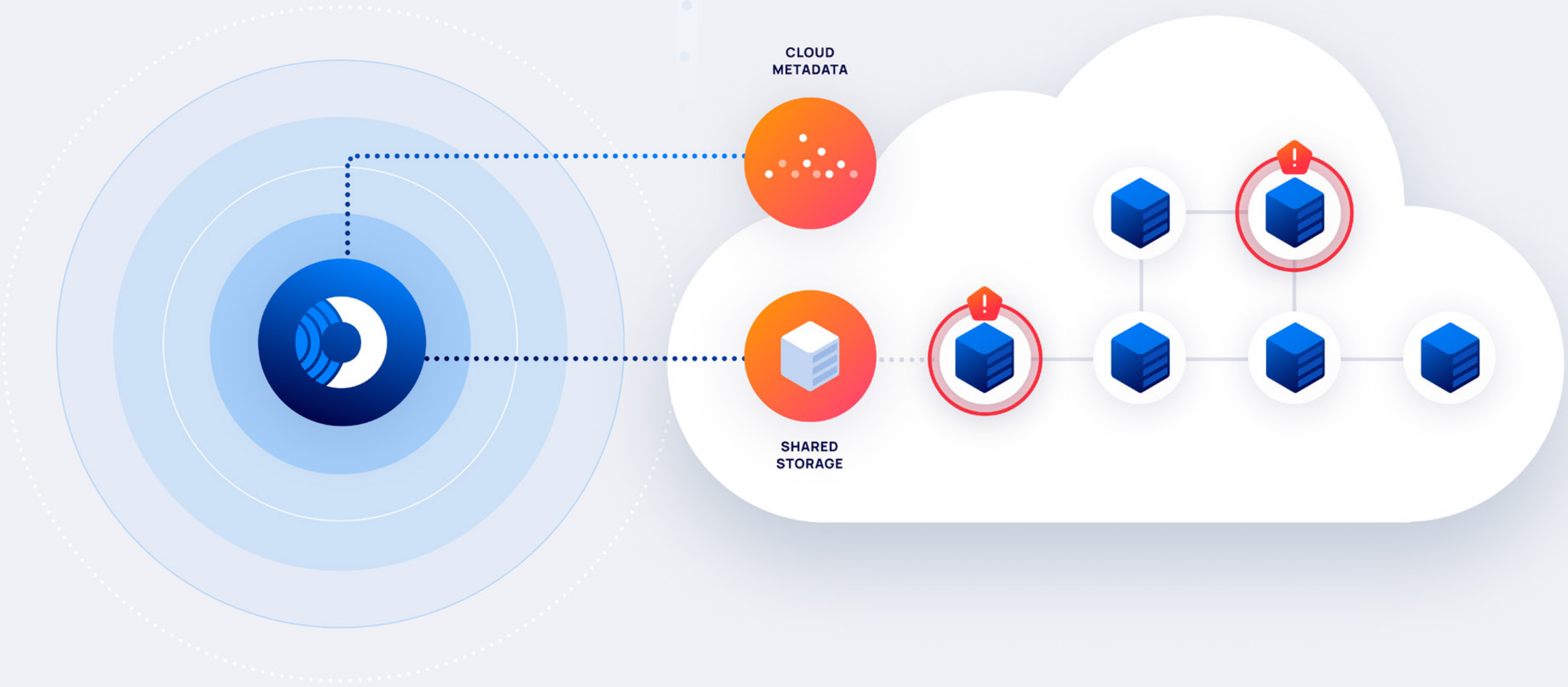
In an effort to solve the cloud security problem, vendors simply applied their existing on-premises technology to the cloud, resulting in many agent-based point solutions that are complex and difficult to manage. Companies, hoping to secure their cloud estate and meet stringent compliance requirements, adopted these solutions, only to find that tedious per-asset integration results in limited coverage, organizational friction, performance degradation, and a high-cost of ownership.

These disparate, siloed tools also diminish the security team's ability to effectively reduce risk. Each tool generates its own alerts without taking into account the overall picture and how cloud assets relate to each other. Alert fatigue ensues as the security team attempts to add the necessary context to tens-of-thousands of security alerts so that they can prioritize remediation efforts.

> Organizations, on average, receive about 10,000 vulnerability alerts for every 100 assets.

Security Built for the Cloud

Orca Security offers a radical new, zero-touch approach to cloud security that eliminates the cost, organizational friction, and performance impact associated with traditional solutions. Orca's patent-pending SideScanning™ technology delivers 100% security visibility and coverage across your entire cloud environment, while a context engine combines workload and cloud configuration details to build a unified data model and visual map of all your assets. Orca's agentless approach and robust capability set replaces many of the point solutions previously needed to secure your cloud estate and maintain regulatory compliance now and in the future.



> "Orca Security provides similar capabilities to what agents on boxes do and more, but with no impact on engineering. It's beautiful. Exactly what I want."

Caleb Sima
VP of Information Security

databricks

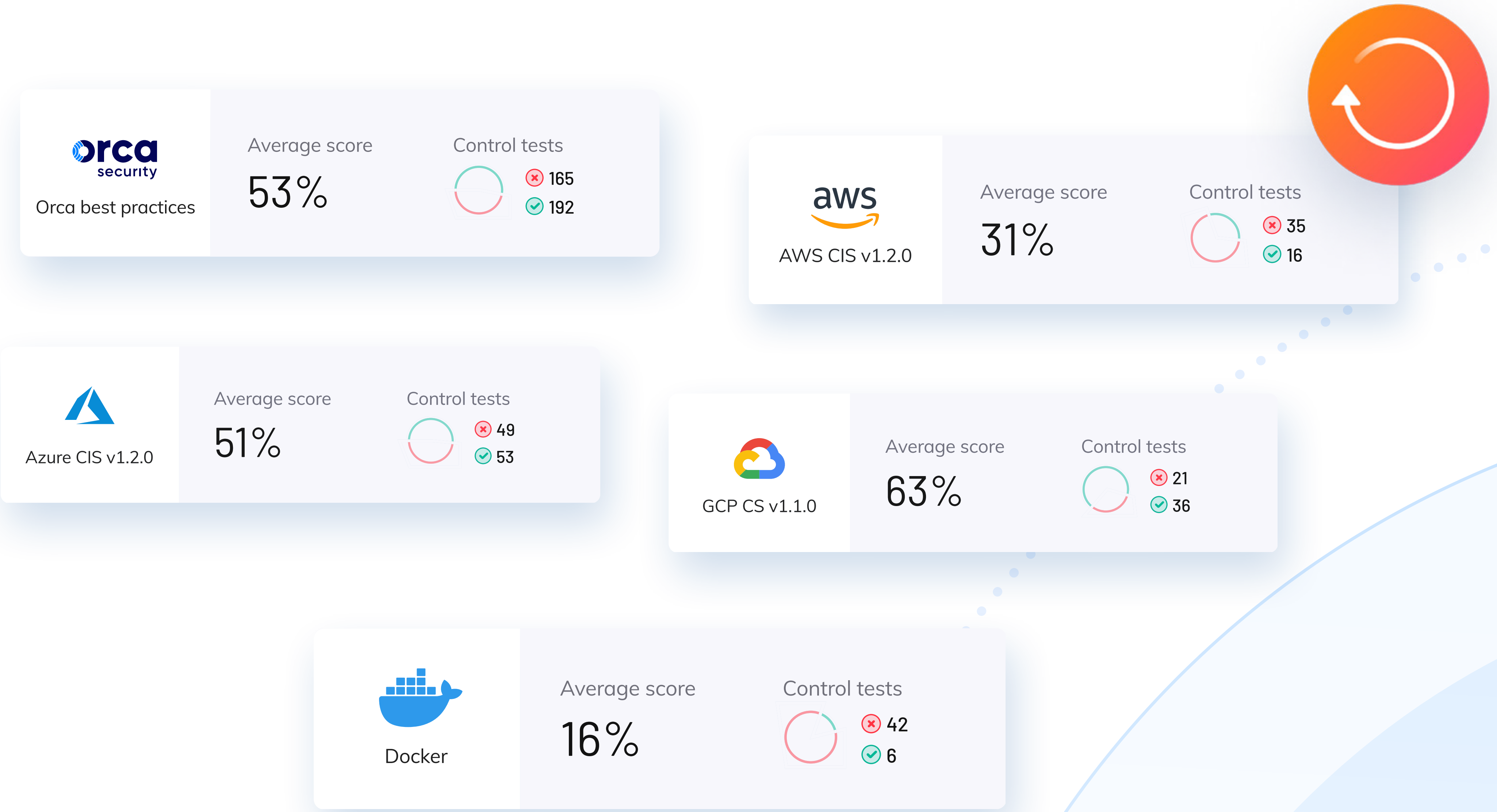
Orca's Context Engine

Unified Data Model

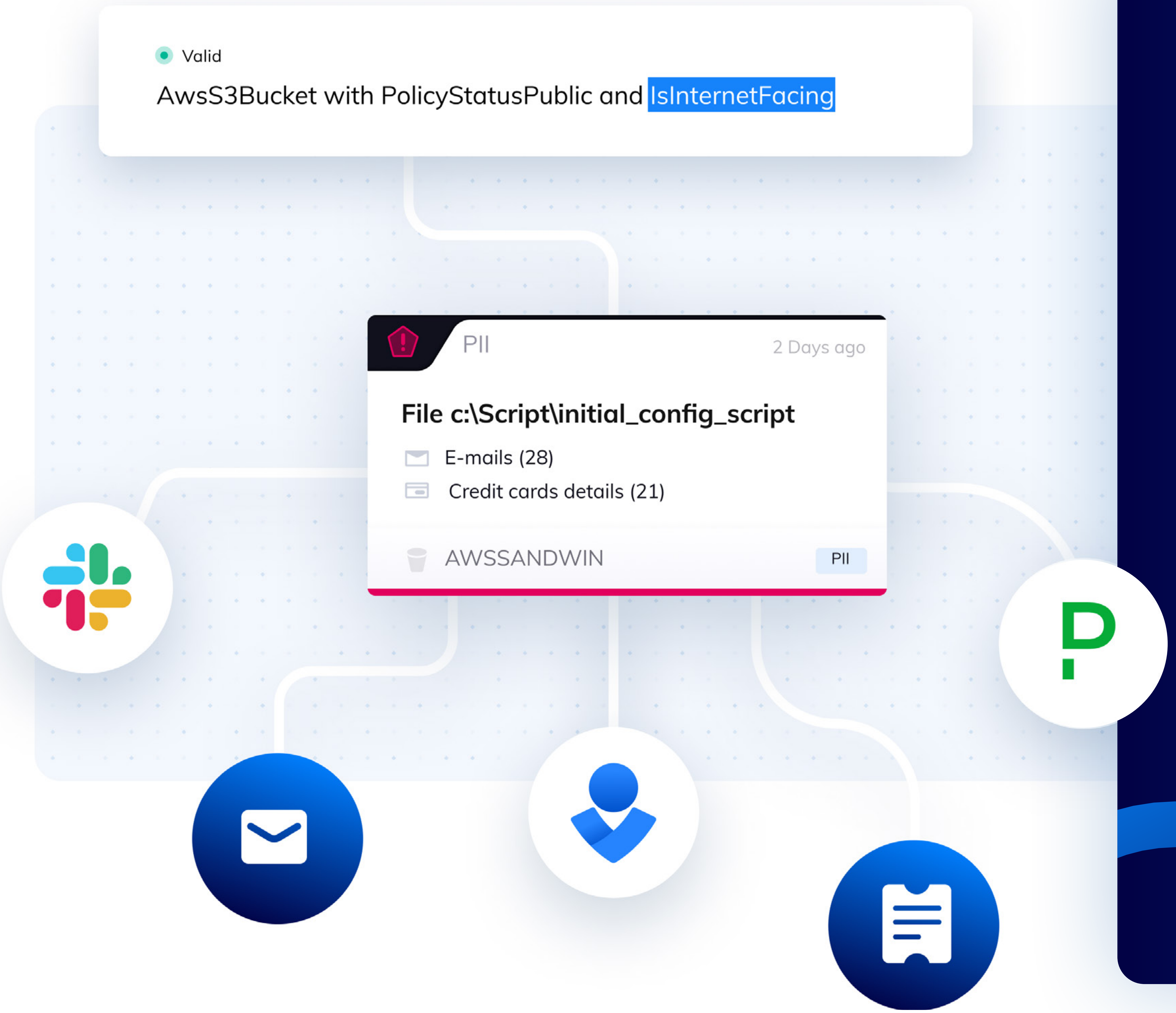
Orca's context engine combines the intelligence gathered from deep inside workloads, including the workload's host configurations (e.g., running services, firewall configurations) with cloud configuration details (e.g., IAM roles, VPCs, security groups) to build a unified data model. This powerful approach 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 measureable improvements to your cloud security posture while avoiding alert fatigue.

Built-in Compliance

With its agentless approach and ability to replace multiple security tools, Orca allows teams to maintain continuous compliance across their entire cloud estate. Orca automatically runs all the critical checks required to maintain continuous compliance with over 35 regulatory and industry frameworks, including a wide range of CIS control benchmarks.



	Average score	Control tests
orca security Orca best practices	53%	☒ 165 ✓ 192
aws AWS CIS v1.2.0	31%	☒ 35 ✓ 16
Azure CIS v1.2.0	51%	☒ 49 ✓ 53
GCP CS v1.1.0	63%	☒ 21 ✓ 36
Docker	16%	☒ 42 ✓ 6



● Valid

AwsS3Bucket with PolicyStatusPublic and IsInternetFacing

PII 2 Days ago

File c:\Script\initial_config_script

E-mails (28)

Credit cards details (21)

AWSSANDWIN PII

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 16 out-of-the-box third-party integrations, including Slack, OpsGenie, Jira, and ServiceNow, Orca helps maximize your organization's productivity. The platform also offers full query and automation capabilities that include auto-ticketing to optimize collaboration and minimize friction between security, DevOps, and remediation teams.

PLATFORM OVERVIEW

Turning Cloud Security on its Side

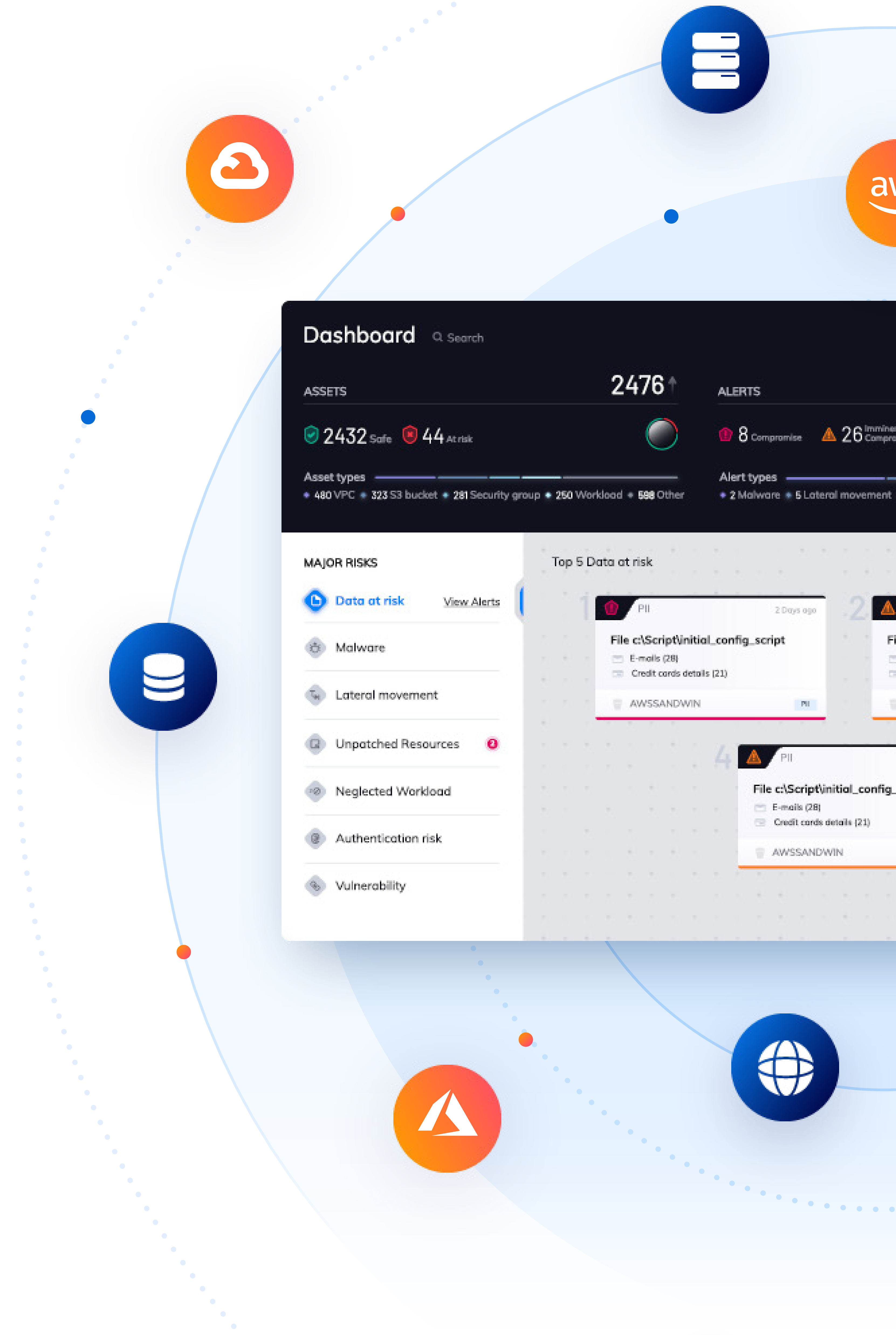
Orca's SideScanning detects critical security issues across your entire cloud estate, including your VMs, containers, and serverless as well as all your cloud infrastructure resources like storage buckets, security groups, VPCs, IAM roles and permissions, KMS keys, and much more—all without sending a single packet over the network or running a single line of code in your environment.

Unlike agents, which sit inside your workloads, SideScanning collects data, with read-only access, from the workloads' runtime block storage. Orca then combines this data with cloud configuration metadata collected via APIs to build a fully contextualized asset inventory and perform a holistic security assessment of your entire cloud estate. All of this is done without any performance impact to your workloads.

After a quick 30-minute deployment process and initial scan, Orca surfaces the most critical security risks that threat actors use or exploit—vulnerabilities, misconfigurations, malware, exposed data, secrets, weak passwords, and lateral movement risk.

> Orca takes daily snapshots from outside your running environment, so there's no downtime, no risk to operations, and no lost data.

Because the **Orca platform detects security risks at every layer of the cloud estate**, it can replace many existing solutions, including vulnerability management, Cloud Workload Protection Platforms, and Cloud Security Posture Management solutions.



Orca delivers the following capabilities through a **single integrated platform**:

- ✓ Vulnerability Management
- ○ Misconfiguration Detection
- ○ Malware Detection
- ○ Lateral Movement Risk Detection
- ○ IAM Risk Detection
- ○ At-Risk Sensitive Data Detection
- ○ File Integrity Monitoring
- ○ Cloud Asset Inventory

1

Vulnerability Management

Using SideScanning, Orca creates a software inventory of your cloud estate to detect vulnerabilities without impacting performance. The software inventory includes information on OS packages, applications, libraries, and other identifying characteristics. Orca uses this information to search for known vulnerabilities in the Orca Vulnerability Database, which includes aggregated data from over 20 vulnerability data sources. Each vulnerability comes with an asset map that visualizes the relationships between individual assets to provide contextualized, prioritized alerts for faster remediation.

← ● ○ ○ ○ ○ ○ ○ ○ →

Orca delivers the following capabilities through a **single integrated platform**:

- ✓ Vulnerability Management
- ✓ Misconfiguration Detection
- ○ Malware Detection
- ○ Lateral Movement Risk Detection
- ○ IAM Risk Detection
- ○ At-Risk Sensitive Data Detection
- ○ File Integrity Monitoring
- ○ Cloud Asset Inventory

2

Misconfiguration Detection

Orca leverages workload and cloud account configuration data to discover and prioritize misconfigurations across your entire cloud estate. Orca supports over 600 unique configuration controls across 35 compliance frameworks. Every configuration control can generate an automated alert to help you improve your security posture and ensure continuous compliance.

Orca delivers the following capabilities through a **single integrated platform**:

- ✓ Vulnerability Management
- ✓ Misconfiguration Detection
- ✓ Malware Detection
- ○ Lateral Movement Risk Detection
- ○ IAM Risk Detection
- ○ At-Risk Sensitive Data Detection
- ○ File Integrity Monitoring
- ○ Cloud Asset Inventory

3

Malware Detection

Orca provides complete malware coverage of your cloud estate, including idle, paused, and stopped workloads, orphaned systems, and devices that can't support agents — with zero performance impact. Orca takes snapshots from outside your running environment and scans cloud assets for malware using a variety of techniques. In addition to signature-based detection, Orca uses advanced heuristic methods such as file analysis, file emulation, and generic signature detection.

Orca delivers the following capabilities through a **single integrated platform**:

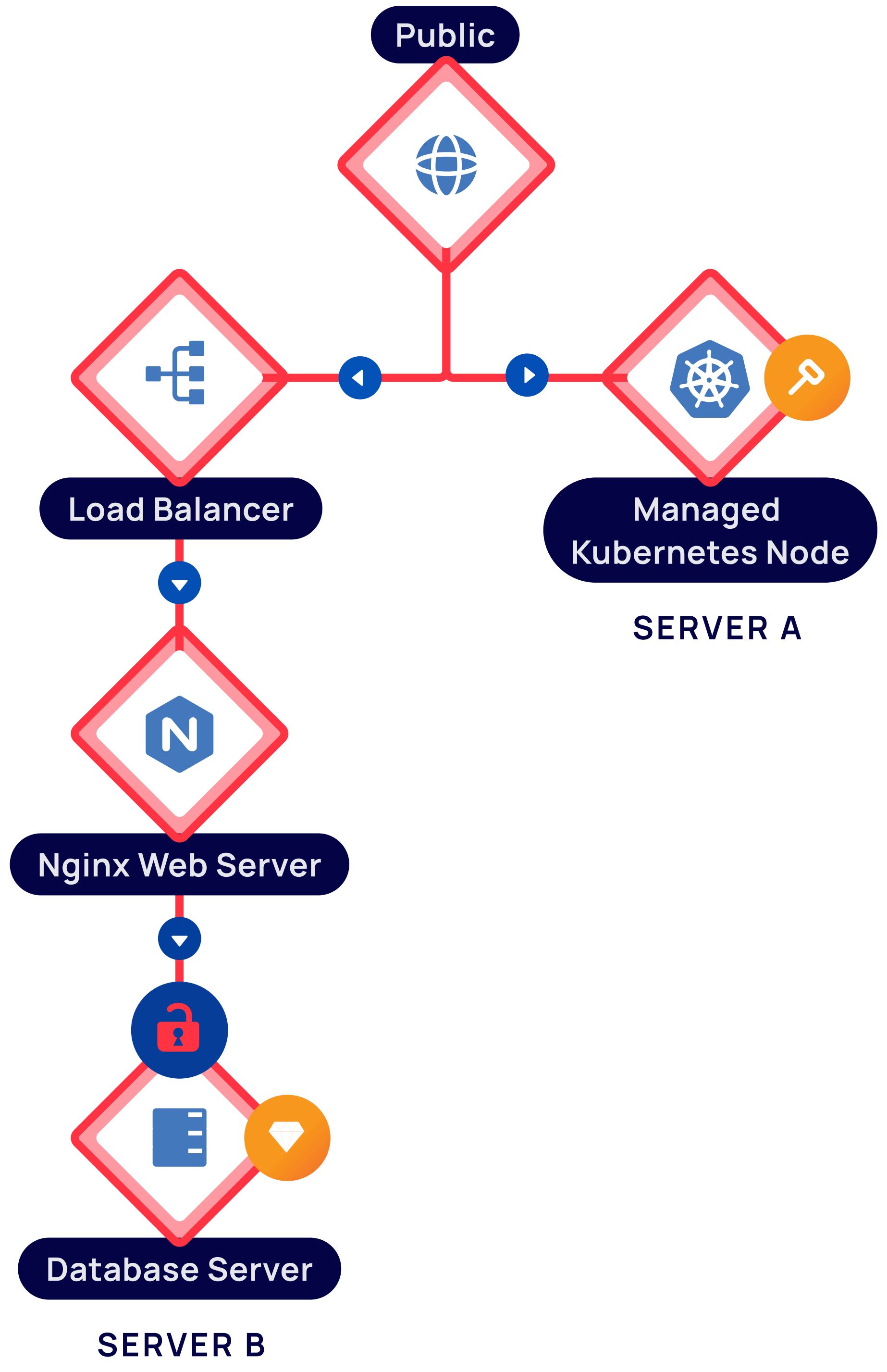
- ✓ Vulnerability Management
- ✓ Misconfiguration Detection
- ✓ Malware Detection
- ✓ Lateral Movement Risk Detection
- ○ IAM Risk Detection
- ○ At-Risk Sensitive Data Detection
- ○ File Integrity Monitoring
- ○ Cloud Asset Inventory

4

Lateral Movement Risk Detection

Orca detects risks and vulnerabilities that could enable lateral movement in your cloud estate and recommends remediation steps to help strengthen your security posture.

Consider the following scenario: Servers A and B never communicate with one another, yet Server A has a key that allows root access to Server B. Most tools would fail to report lateral movement risk because there is no traffic between the two machines. However, Orca would detect this risk because it is contextually aware of the connections between the assets.



Orca delivers the following capabilities through a **single integrated platform**:

- ✓ Vulnerability Management
- ✓ Misconfiguration Detection
- ✓ Malware Detection
- ✓ Lateral Movement Risk Detection
- ✓ IAM Risk Detection
- ○ At-Risk Sensitive Data Detection
- ○ File Integrity Monitoring
- ○ Cloud Asset Inventory

5

IAM Risk Detection

Orca detects, prioritizes, and continuously monitors for common and obscure Identity and Access Management (IAM) misconfigurations across your public cloud to meet stringent IAM compliance mandates and improve your cloud security posture. In addition to poor password hygiene, Orca scans your cloud for exposed keys, passwords in shell histories, vulnerabilities, and other information attackers can use to move laterally in your environment.

Orca delivers the following capabilities through a **single integrated platform**:

- ✓ Vulnerability Management
- ✓ Misconfiguration Detection
- ✓ Malware Detection
- ✓ Lateral Movement Risk Detection
- ✓ IAM Risk Detection
- ✓ At-Risk Sensitive Data Detection
- ○ File Integrity Monitoring
- ○ Cloud Asset Inventory

6

At-Risk Sensitive Data Detection

Orca detects at-risk sensitive data across both the workload and control planes. This includes improperly secured Personally Identifiable Information (PII) such as email addresses, credit card numbers, and Social Security identifiers. Orca pinpoints the data's exact location and provides masked samples for quick triage and remediation. Alerts are prioritized based on context such as the location and accessibility of the assets containing the data. This approach reduces false positives and the alert fatigue common with at-risk data detection.

Orca delivers the following capabilities through a **single integrated platform**:

- ✓ Vulnerability Management
- ✓ Misconfiguration Detection
- ✓ Malware Detection
- ✓ Lateral Movement Risk Detection
- ✓ IAM Risk Detection
- ✓ At-Risk Sensitive Data Detection
- ✓ File Integrity Monitoring
- ○ Cloud Asset Inventory

7

File Integrity Monitoring

Orca's agentless File Integrity Monitoring (FIM) monitors a set of critical files on your Linux and Windows workloads. Orca discovers and classifies any changes or drift from an established baseline and provides you with key remediation information, helping you to comply with regulations and standards, such as PCI-DSS, that require FIM.

← ○ ○ ○ ○ ○ ○ ● ○ →

Orca delivers the following capabilities through a **single integrated platform**:

- ✓ Vulnerability Management
- ✓ Misconfiguration Detection
- ✓ Malware Detection
- ✓ Lateral Movement Risk Detection
- ✓ IAM Risk Detection
- ✓ At-Risk Sensitive Data Detection
- ✓ File Integrity Monitoring
- ✓ Cloud Asset Inventory

8

Cloud Asset Inventory

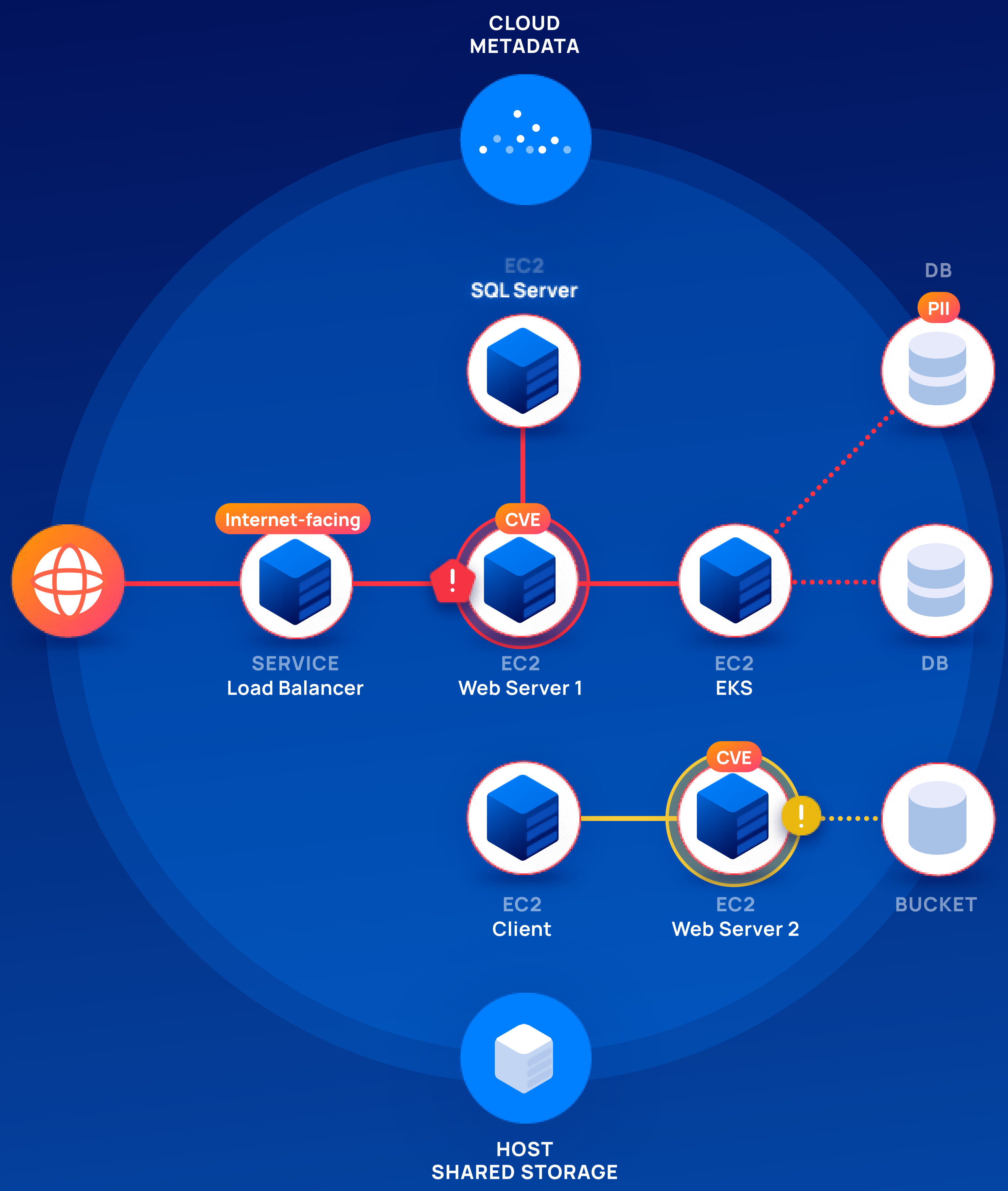
Orca performs a complete inventory of your public cloud assets, including software inventories of cloud workloads. It also inventories assets on your cloud infrastructure platform, including data and network assets such as storage buckets, security groups, cloud accounts, images, cloud services, and more. Orca's powerful query capabilities simplify searches for assets and resources (e.g., "all externally facing hosts that have a specific CVE vulnerability and a certain port open").

Next Page

Intelligence Powered by Context

Understanding risk in context is critical. It's the difference between effective security and alert fatigue. Most solutions available today only consider the severity of the underlying security issue (e.g., CVSS score) and dismiss accessibility (e.g. how accessible is the risk) and the potential business impact if the risk is exploited.

Orca approaches risk scoring contextually by considering all three risk variables. It then calculates a severity score for every potential threat, based on context, allowing it to separate the "imminent dangers" from the "potentially hazardous warnings." Each risk is enriched with the context necessary to help security operations teams focus on fixing what matters most.



EXAMPLE

Server 1 and Server 2 are both Apache web servers. They are both using a vulnerable library (CVE-2018-1176). Available solutions will simply report this vulnerability with a static score, with both servers receiving the exact same score of 8.8.

Orca's context engine sees from the cloud configuration data that Server 1 is Internet-facing and is easily accessible to attackers, prioritizing it as "imminent compromise." Server 2 is an intranet server that is not publicly accessible and poses a minimal threat to the organization. Therefore, it is categorized as "hazardous" only.

About Orca Security

Orca Security, the cloud security innovation leader, provides instant-on security and compliance for AWS, Azure, and GCP—without the gaps in coverage, alert fatigue, and operational costs of agents.

Give your team superpowers and simplify security operations with a single SaaS-based cloud security platform for workload and data protection, cloud security posture management, vulnerability management, and compliance management. Instead of disparate tools operating in silos, Orca Security builds a graph that encompasses all cloud assets, software, connectivity, and trust—then prioritizes risk based on the severity of the underlying security issue, its accessibility, and business impact. This eliminates thousands of meaningless security alerts and helps you focus on what matters most.

With Orca Security, no code runs within your cloud environment. Orca SideScanning™ reads your cloud configuration and workloads' runtime block storage out-of-band, detecting vulnerabilities, malware, misconfigurations, lateral movement risk, weak and leaked passwords, and unsecured PII. There are no overlooked assets, no DevOps headaches, and no performance hits on live environments.

Visit https://orca.security

Trusted by Organizations
Around the Globe

fiverr.
Lemonade
Robinhood
druva
databricks
BeyondTrust
unity
LiveOakBank.

orca security

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