



The Ultimate Guide to AWS Cloud Asset Visibility

How traditional vulnerability management, cloud workload protection, and cloud security posture management solutions compare to Orca's cloud-native application protection platform for visibility across your Amazon Web Services (AWS) cloud estate.



Synopsis

It's no secret that AWS deployments are skyrocketing globally, with organizations of all sizes and industries transitioning more and more of their infrastructure and assets to the cloud. Are enterprises managing to keep their complex and ever-expanding cloud estates secure? The answer is: No. According to IDC, in 2021, 98% of companies experienced a cloud data breach in the previous 18 months, up from 79% in 2020¹.

Cloud security starts with full visibility of your cloud estate. However, conventional security tools have blind spots. They either don't see all of your assets or can't analyze them in depth. There is, however, a next-generation cloud security solution that delivers in-depth, full-stack visibility into AWS without agents.

This ultimate guide covers the pros and cons of current cloud security solutions and includes a comprehensive comparison table. It concludes with what the future holds for gaining deeper visibility into your AWS cloud estate.



¹ Ermetic Reports Nearly 100% of Companies Experienced a Cloud Data Breach in Past 18 Months (yahoo.com).

Introduction

According to [Gartner](#), by 2023, 70% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 40% in 2020. First seen as a cost-saving strategy, companies are now also leveraging the cloud to accelerate IT service delivery, improve business continuity, and provide greater flexibility, resulting in competitive advantages in dynamic market conditions.

However, as cloud environments continue to expand at an unprecedented rate, new security risks arise. In an effort to reduce time to market, development teams routinely deploy new assets, unbeknownst to security teams. Organizations need a solution that lets DevOps teams experiment and innovate without having to worry about deploying security measures such as agents, while still giving security teams full-stack visibility into all cloud assets.



Full-stack visibility provides a complete understanding of what goes on inside the AWS environment: the infrastructure level, operating systems, applications, and data.

Full-stack visibility across four layers

Full-stack visibility of the AWS cloud environment is even more challenging when attempting to combine agent-based systems with first-generation cloud security posture managers. This patchwork of non-cloud-born solutions and their workflows is operationally cumbersome and simply does not provide complete coverage of cloud assets, leaving organizations with potentially unseen and unmitigated risks in their cloud environments.

According to Gartner, "Through 2025, more than 99% of cloud breaches will have a root cause of customer misconfigurations or mistakes."² Gaining visibility into your AWS cloud configurations is therefore crucial in order to maintain a secure AWS environment.

The OS and application layers are the most critical, as they are the most commonly targeted attack surfaces in the cloud today.

² Gartner, Inc., "Cool Vendors in Cloud Security Posture Management," Tom Croll, Neil MacDonald, Mark Wah, Prateek Bhajanka, June 9, 2021.

1

Infrastructure Level

All assets run on top of this layer. Clear visibility into this layer provides answers to the following questions: Which assets are running on which networks? Who is allowed to access them?

2

Operating System Level

Common issues like remote code execution vulnerabilities exist in this layer. It is vital to see which OS is in use and when it was last updated or patched. Is it secured sufficiently, or is it wide open? What is the configuration setup? Are user privileges in compliance? Have all required patches been applied?

3

Application Level

This layer is where the vast majority of vulnerabilities reside. One example of a breach at the application level is the 2017 breach at Equifax that exposed the personal information of nearly 150 million consumers, resulting in up to \$700 million in fines and compensation. It is vital to see all installed applications and their configurations, as well as know if they've been patched appropriately.

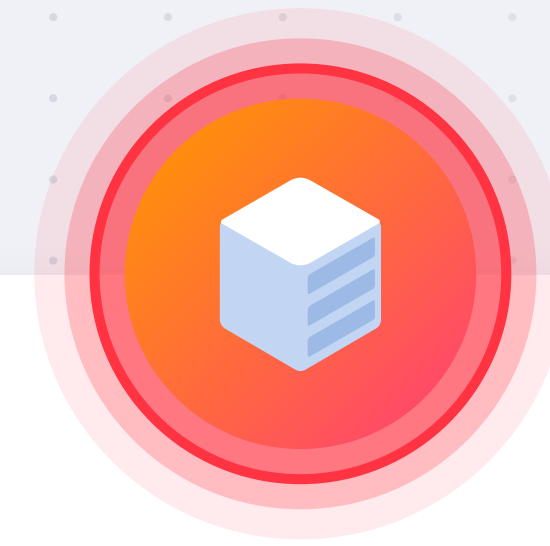
4

Data Stack Level

This layer includes an inventory of all data and where it is stored. Clear visibility into this layer is critical for determining where the organization's crown jewels are and which servers include sensitive data such as personally identifiable information (PII) or payment data.

Security Risks of AWS Deployments

Cloud adoption commonly creates friction between security teams and other departments in the organization. DevOps teams should be free to innovate unhindered in the cloud, and security teams must be able to protect corporate assets. Uncertainty about roles and responsibilities causes organizational friction between DevOps, IT, and security and can result in unpatched vulnerabilities, unmanaged assets, and misconfigured or abandoned user accounts.



Cloud assets can be very dynamic as they are spun up and torn down on demand, which makes them difficult to track and manage. **Due to the tremendous efforts required to deploy them**, traditional non-cloud-born cloud security solutions don't provide complete visibility. As a result, they cannot reliably answer basic questions such as:

- ✓ Do I have servers vulnerable to XYZ?
- ✓ How many of my servers are running ABC?
- ✓ Is any of my sensitive data stored insecurely?
- ✓ How many versions of this database exist?
- ✓ Which assets with XYZ vulnerability are internet facing?

Below we have listed the cloud layers and a breakdown of their specific security concerns:


CLOUD LAYERS	DESCRIPTION	VISIBILITY NEEDS	EXAMPLE SECURITY CONCERN
Infrastructure Level	Defines who can access the machine (IAM users and roles), the networks it is connected to, logging policies, and disk-level encryption.	Who has access to the machine (avoiding possible misconfigurations), connections to the wrong or dangerous networks.	An internal server that’s mistakenly connected directly to an external network.
Operating System Level	Manages, operates, and executes processes.	Inventory of OS services, as well as vulnerabilities, including updates and patch status, configurations, and misconfigurations.	Weak authentication configuration that puts the machine in jeopardy or open ports; vulnerabilities residing in OS services, such as PrintNightmare.
Application Level	Applications installed on the machine, such as web servers, CRMs, databases.	Application inventory, as well as vulnerabilities within all versions of the apps, configuration, or security misconfigurations of the apps, and the existence of malicious code, which would leave you with a compromised machine.	Vulnerable web servers, databases, or even malware such as a crypto mining script that is attached to an application.
Data Stack	The data that is used by applications, such as database content.	Ability to answer, “Where is my PII stored?” and “What critical data exists on these assets?”	Stored credit card information or other PII.

Conventional Cloud Asset Visibility Solutions

The most common cloud security solution types that provide visibility into the AWS cloud include:

- Cloud workload protection platforms (CWPP)
- Cloud security posture management (CSPM) solutions

Both solutions have their distinct pros and cons. The following chart breaks down each type of solution and its capabilities.

CLOUD SECURITY PLATFORM CAPABILITIES	CWPP	CSPM	
Risk to scanned assets	 Medium	 None	 None
Operating cost	 High	 None	 None
Security visibility (depth)	 Medium	 Very Low	 High
Security visibility (breadth)	 Low	 Medium	 High
Workload OS support	 Medium	 None	 High
Can be circumvented by malware	 Yes	 Yes	 No
Performance impact	 Moderate	 None	 None
Vulnerability detection	 Yes	 Limited (can't scan workloads)	 Yes
Malware detection	 Yes	 Limited (can't scan workloads)	 Yes
Full stack asset inventory	 Limited (no cloud infra)	 Limited (no software inventory)	 Yes
Cloud level misconfiguration detection	 No	 Yes	 Yes
Physical system support	 Yes	 No	 No
Scan stopped machines	 No	 No	 Yes



1. Agent-based Solutions

Most CWPPs use agents to gain insight into cloud workloads. Agent-based CWPP solutions require software agents to be installed on every asset. Qualys Cloud, Rapid7 Insight, and Tenable.io are some of the more popular agent-based solutions available.

How they work

Agent-based solutions require an agent to be installed, sometimes manually, on each asset to be monitored. The agent scans the host and sends results back to a management service.

Maintenance

The agent must communicate with the management service to report its findings, which requires constant monitoring as well as occasional software updates.

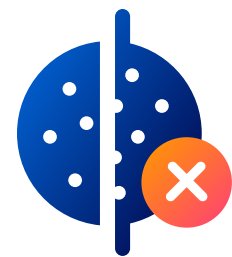
Due to cumbersome and partial deployments, agent-based solutions can't reliably provide full visibility.

PROS

- Delivers in-depth visibility into issues within the OS, applications, and data by examining files, processes, and registry data.
- Detects malware and vulnerabilities on the host.
- Can provide continuous visibility.

CONS

- Very high TCO due to the necessity of administering continuous updates, individually installing agents for each asset, and maintaining communication with the management service.
- If agents are not deployed for all assets, this can expose organizations to serious security gaps. On average, we found that less than 50% of assets are covered by host cloud security solutions.
- Impacts workload performance by consuming CPU, memory, and disk space.
- Some operating system versions are not supported by agents.
- Can't access AWS infrastructure resources, such as storage buckets. Agents cover three of the four cloud layers – OS, applications, and data – but they don't scan the AWS infrastructure.



2A. Network Scanners - Unauthenticated

Some CWPPs utilize network scanners to gain insight into the cloud workloads. Similar to agent-based solutions, CWPP network scanning tools attempt to identify possible vulnerabilities on the host. Products in this category include solutions from Qualys, Rapid7 Nexpose, and Tenable Nessus.

Agentless network scanners can be divided into two categories: authenticated and unauthenticated.

How they work

An unauthenticated scanner scans each host for open ports and installed applications. It then tries to determine if the host is susceptible to vulnerabilities by attempting to connect to it and using fingerprinting techniques that are based on how the host responds.

Maintenance

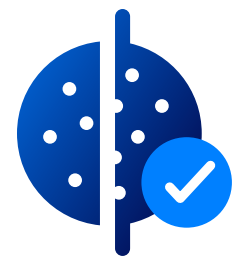
Need to ensure that all AWS workloads are scanned. This is problematic when working in the AWS cloud and new workloads are added frequently.

PROS

- Initial costs are low for partial visibility (but grow significantly with greater coverage).
- Ability to obtain data on vulnerabilities without on-asset installation or authentication.
- Broad security visibility when given suitable access to each network.

CONS

- The scanner can inadvertently cause service outages when trying to connect to a host.
- Due to the fact that they're scanning from the outside, unauthenticated scanners use heuristic techniques in order to determine the OS, OS services, and applications that are installed on the workload. False negatives are a common side effect. An administrator can augment these detection methods by providing the details, but administrators frequently overlook this technique due to operational overhead.
- Unauthenticated network scanners are often blocked by firewalls and IPSs. Making sure the scans are completed correctly requires a lot of manual work, which is impractical due to a large number of networks within the cloud environment.



2B. Network Scanners - Authenticated

Some CWPPs utilize network scanners to gain insight into the cloud workloads. Similar to agent-based solutions, CWPP network scanning tools attempt to identify possible vulnerabilities on the host. Products in this category include solutions from Qualys, Rapid7 Nexpose, and Tenable Nessus.

Agentless network scanners can be divided into two categories: authenticated and unauthenticated.

How they work

An authenticated scanner, also known as a credentialed scanner, uses privileged credentials to log into each host to detect vulnerabilities and security misconfigurations.

Maintenance

Like unauthenticated scanners, authenticated scanners must be deployed on each and every network, which can be problematic when working in the cloud as new networks are frequently added. In addition, providing credentialed access is time-consuming.

PROS

- Provides in-depth security visibility without requiring an agent on each machine.
- Can detect vulnerabilities for issues on the OS, application, and data layers.

CONS

- The requirement to deploy a scanner on each network and integrate with the credential management system can lead to high operating costs and/or partial deployment and reduced visibility.
- Administrators must modify firewalls to allow remote authentication, creating a potential security risk.
- Security is limited to machines that have been given credentialed access to an authenticated network scanner.



3. Cloud Security Posture Management (CSPMs) Solutions

How they work

CSPM solutions are designed to connect to the AWS cloud infrastructure and analyze data about AWS assets, the networks they belong to, user permissions, roles, tags, and more. Products in this category include solutions like Palo Alto Networks (RedLock and Evident.io) and Rapid7 (DivvyCloud).

Maintenance

Continuous checks of AWS platform account compliance can detect misconfigurations, such as assets with inappropriate IAM roles or publicly accessible data stores.

CSPMs don't penetrate the layers above the AWS cloud I/S, failing to provide visibility into OS and application level vulnerabilities and other security risks.

PROS

- Low maintenance and low operational costs.
- Low risk; no agents or proxies are required.
- Sees all AWS infrastructure assets.

CONS

- Limited security visibility depth within each asset, covering the lowest level of the stack. A CSPM cannot provide visibility into the OS, application, or data layers.
- Doesn't use workload security data to help prioritize the criticality of AWS infrastructure security issues.
- While it provides a full list of assets, the data provided on each is limited.

Cons Outweigh the Pros

When comparing conventional solutions, the cons outweigh the pros. Integrating multiple tools can eliminate some of the deficiencies, but more integration requires more time, management, and manpower.

Furthermore, deploying and maintaining multiple solutions is not a cost-effective way to spend the IT budget. Many businesses know all too well that even if they implement multiple solutions there's no guarantee of full visibility or improved security. One or more assets on one of the four layers will almost certainly not be covered. It's also highly likely that the assets with limited visibility are the ones most prone to risks. For example, a department or subcontractor that hasn't followed guidelines to install agents on their assets or integrate them with a credential management system has probably ignored other security measures and guidelines as well.



Integrating multiple tools can solve some of the deficiencies, but the more integration needed, the more time is wasted on management and correlation.



The Orca Agentless Cloud Security Platform

Orca's single, agentless SaaS-based platform delivers cloud workload protection and cloud security posture management, including vulnerability management and compliance, for AWS, without the gaps in coverage, alert fatigue, organizational friction, and operational costs of agent-based solutions. The Orca Cloud Security platform protects AWS workloads including EC2, EKS, ECS, Fargate, and Lambda as well as finding configuration issues in the native services.

Orca Security collects data, with read-only access, from AWS workloads' runtime block storage out-of-band and combines this data with cloud configuration metadata retrieved via AWS APIs to detect risks across both the workload and control plane.

Customers can easily scan S3 buckets for personally identifiable information (PII) and malware without moving or storing the underlying data. Orca Security also enables AWS customers to leverage CloudTrail events to trigger new scans and update risk levels as configurations change in near real time. With Orca Security, customers can inspect Identity Access Management (IAM) policies, generate alerts, and visualize issues via an access risk map.



How it works

After a quick, 30-minute deployment process and initial scan, Orca surfaces the most critical security risks that threat actors exploit, like vulnerabilities in operating systems and applications – including the components that make up applications, namely packages and libraries.

Orca detects misconfigurations and malware, even on neglected orphaned workloads that have flown under the radar, as well as those that haven't been maintained for years.

Orca can also detect the risk of lateral movement, in particular workloads with keys that can be used to access other sensitive resources. We see this often – such as forgotten cloud keys that provide root access due to poor security hygiene – or secure shell keys that facilitate access to the entire AWS environment.

Intelligence Powered by Context

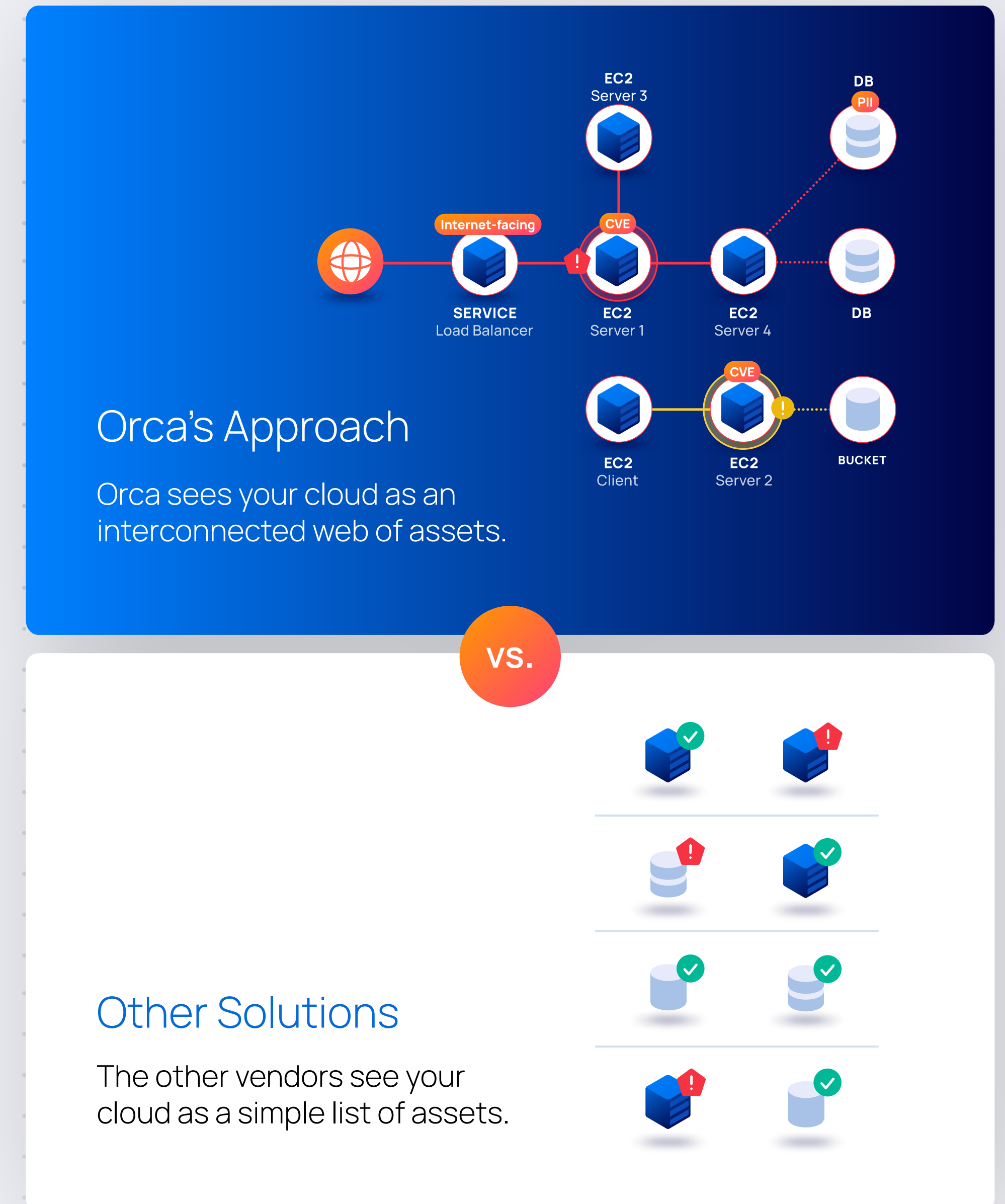
Combining the intelligence from the workload (workload plane) with AWS metadata (control plane) enables Orca to obtain complete visibility into your entire AWS cloud estate, as well as understand the connection between different assets. With this visibility, Orca builds the context necessary to truly understand your AWS environment in its entirety. This approach facilitates an immediate understanding of all the significant risks in the environment and their relative importance.

Because we detect every important security risk at every layer of the AWS environment (workload + control plane), we see not just the workload, but also its location and context. We can see if it's connected to an internal vs. external network, which ports are open on the firewall protecting it, and much more. Moreover, other solutions only consider one dimension of risk: the severity

of the underlying security issue. This invariably results in a large number of alerts that lack context and prioritization, causing alert fatigue and requiring security teams to waste valuable time assessing the priority of each issue.

Unlike other solutions that take a narrow view of risk, we see it multi-dimensionally. Risk involves not only the severity of the underlying security issue, but also its accessibility (how accessible is the risk), and its blast radius (what is the potential impact to the business).

This results in effective prioritization of critical alerts, dramatically reducing the time needed to sift through large volumes of alerts and determines which alerts are truly critical and which are false positives. We have found that Orca reduces alerts **by 99.9%** compared to other solutions.

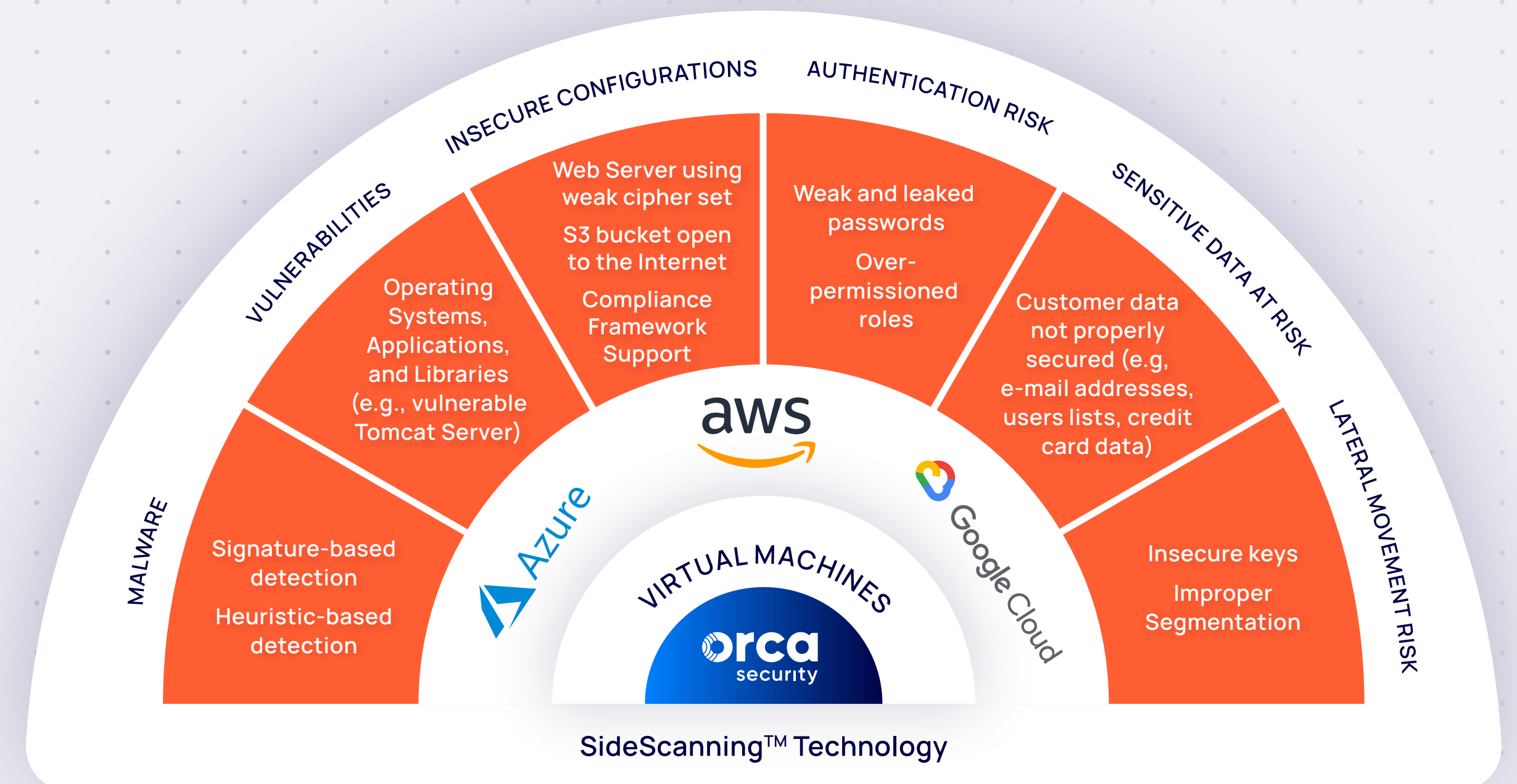


Multiple Tools in One Platform

Orca reduces operational costs and improves effectiveness by providing a single platform with the core capabilities of CSPM and CWPP, including vulnerability management and compliance. This allows security teams to get a complete picture of the security and compliance issues across your AWS cloud estate without having to manually correlate data from disparate tools.

Orca further helps organizations improve efficiency and expedite remediation by allowing security teams to prioritize, customize, and integrate automated alerts into existing workflows. This allows you to automatically process high volumes of AWS security data, leaving you with more time to devote to higher-value activities.

Major Risks Covered



Ease of Deployment

In a matter of minutes, Orca provides full-stack visibility into the security posture of all assets in your entire AWS footprint. There is no need to constantly monitor or integrate new systems. As it leverages read-only integration, there is no risk involved. Given that Orca detects every important security risk at the cloud infrastructure, OS, application, and data layers of your AWS cloud estate, it can replace multiple solutions — such as legacy vulnerability assessment tools, as well as CSPM and CWPP solutions — which reduces operational costs and improves return on investment.

SideScanning™ provides full stack visibility into all of your AWS assets.

PROS

- Full-stack visibility into all of your assets in minutes. It can even scan paused, stopped, and idle machines.
- Deep security visibility on vulnerable software, non-secure configurations, and compromised assets.
- Leverages context-aware intelligence to recognize when seemingly unrelated issues can be combined to create dangerous attack paths.
- Utilizes read-only access, so there is no performance or availability impact.
- Provides full-stack asset inventory for your entire AWS deployment. Not a single asset is missed.
- Enables security teams to do their job without the enormous costs and organizational friction involved in deploying agents or network scanners.
- One-time integration to the cloud infrastructure level covers all assets, no matter how many exist.
- Since it doesn't rely on the scanned machine, Orca's SideScanning™ solution can detect rootkits and malware that can circumvent security agents.

CONS

- Does not currently cover Internet of Things devices.
- Does not support bare metal environments.



Orca and AWS: Better Together

As an Amazon Web Services ISV Partner, we're committed to working closely with you to secure your AWS cloud estate. Orca Security's commitment and support for AWS include:

AWS Marketplace: Customers can procure Orca on the [AWS Marketplace](#) and use their AWS spending commitments.

AWS Security Competency: Orca is technically validated by AWS for its sound architecture, adherence to AWS best practices, and expertise within the cloud security space.

AWS Linux 2 Service Ready: Orca supports AWS Amazon Linux and Amazon Linux as a platform of discovery.

AWS CIS Compliance Benchmarks: Orca fully adheres to the Center for Internet Security (CIS) benchmarks for AWS cloud infrastructure.

AWS PrivateLink Support: Orca integrates with this AWS API ensuring private connectivity between VPCs and services hosted on AWS without exposing any data to the Internet.

AWS Image Builder Integration: With AWS Image Builder, Orca can integrate with your CI/CD pipeline, making sure your DevOps teams are shipping hardened and verified images to production.

AWS Activate: Commence your startup journey with cloud security and compliance by leveraging [Orca Security's AWS activate startup offer](#). Qualified startups will receive 100 AWS workloads for free for one full year or until your next funding round.

"Orca took half an hour to set up and fully deploy for the POC. It was nothing to get it going, Jaffe says. We saw results immediately. In under 24 hours, we could see all the resources and the environment in all of our AWS accounts."



Jonathan Jaffe
CISO, Lemonade

Read the [full story](#)

Conclusion

While conventional cloud security solutions have their strengths, when it comes to AWS visibility, it's clear that no matter which one is implemented, there will always be something missing in AWS coverage. Even when deploying a combination of agents, network scanners, and CSPMs, there will still only be partial visibility. In most cases, organizations manage to reach less than 50% coverage when using these methods.

Orca's agentless cloud security platform is the next generation, comprehensive solution for providing full-stack visibility into AWS assets.

Find us on the AWS Marketplace

For more product details and to read customer reviews, visit us on the [AWS Marketplace](#). Or, [browse more resources](#) to learn how you can achieve complete security coverage for your AWS cloud environment.

For more information on the Orca Security Platform

Contact: info@orca.security

"We have 12 AWS accounts. We didn't know what was in all of them, so we plugged them into Orca. Within 30 minutes we had a good idea of what was running in all accounts. We couldn't have done that so quickly any other way."



Jeremy Turner

Senior Cloud Security Engineer,
Paidy

Read the [full story](#)



About Orca Security

Orca Security, the cloud security innovation leader, provides instant-on security and compliance for public cloud estates — without the gaps in coverage, organizational friction, alert fatigue, and operational costs of agents.

Give your team superpowers and simplify security operations with a single [CNAPP platform](#) for workload and data protection, cloud security posture management, vulnerability management, and compliance. Instead of disparate tools operating in silos, Orca Security builds a graph that encompasses all AWS 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 AWS environment. Orca SideScanning™ reads your AWS 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.

Orca Security is trusted by global innovators, including Databricks, Lemonade, Druva, and Robinhood. Connect your first AWS account in minutes and see for yourself.

[Visit Orca Security](#)

“Within minutes, we gained full visibility into our AWS account. Before Orca, I had zero visibility. Now, I see everything I need to see. Plus, we now have a single tool that does it all.”



Shahar Maor
CISO, Fiverr

[Read the full story](#)