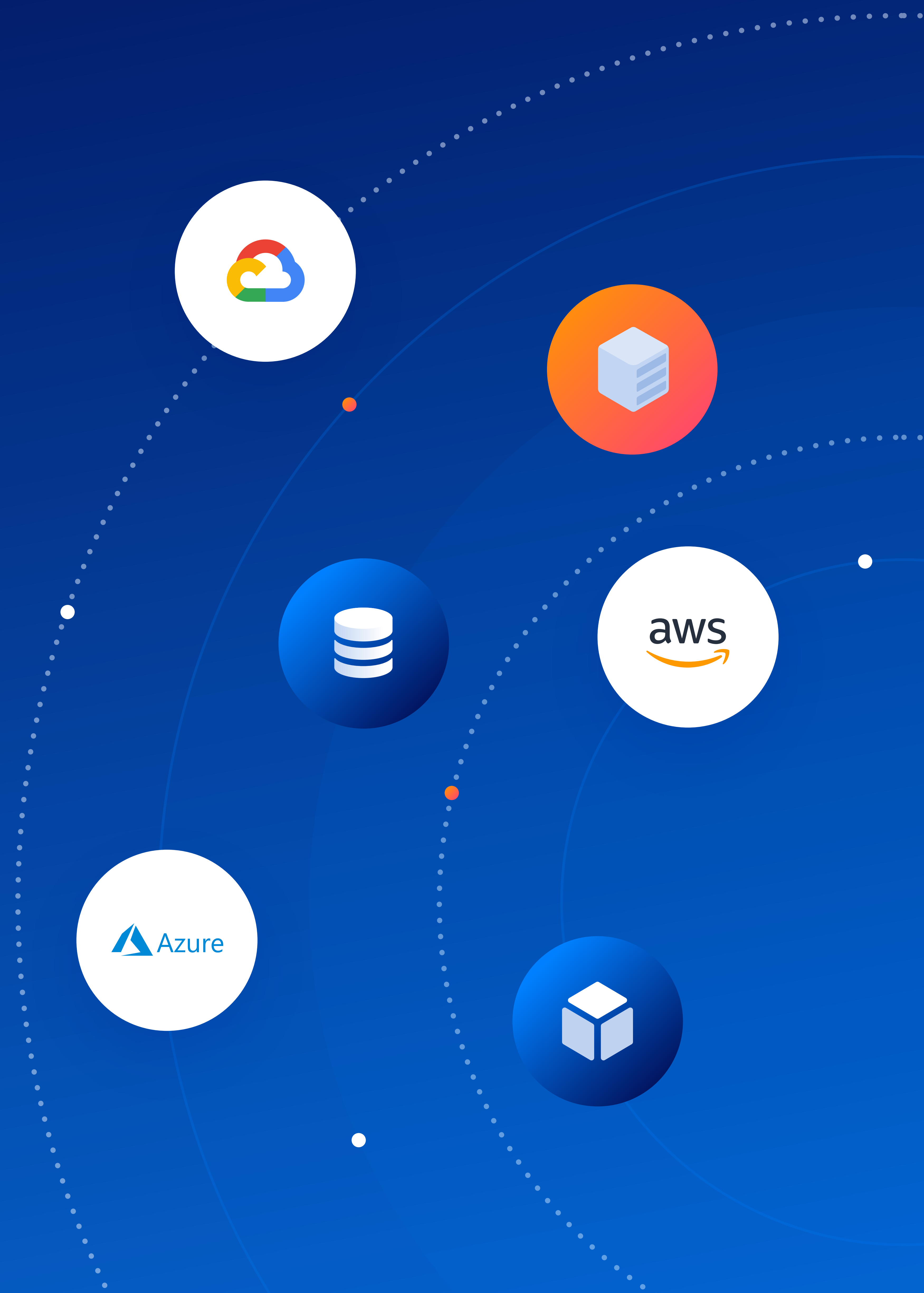
orca security

The Ultimate Guide to AWS, Azure, and GCP Cloud Asset Visibility

How traditional vulnerability management, cloud workload protection and cloud security posture management solutions — compare to Orca's agentless cloud security platform for visibility across your entire cloud estate.



Synopsis

It's no secret that cloud deployments are skyrocketing globally, with organizations of all sizes and industries transitioning at least some of their infrastructure and assets to the cloud. Are enterprises managing to keep up with the security and visibility of their complex and ever expanding cloud estates? The answer is: no.

Conventional security tools all have blind spots. They either don't see all cloud assets or can't analyze assets in depth. There is, however, a new-generation cloud security solution that delivers in-depth, full-stack visibility into AWS, Azure, and GCP without agents.

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

Introduction

According to the 2020 IDG Cloud Computing Study, 81% of organizations have deployed at least a portion of their computing infrastructure in the cloud. First seen as a cost-saving strategy, companies are now 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 improve market responsiveness, development teams routinely leave security teams out of the loop when it comes to new asset deployments. This is not, of course, a calculated plan to sabotage company security. Rather, speed is of the essence, so security often takes a back seat in the rush to market. Organizations need a solution that lets DevOps teams work without worrying about deploying visibility measures such as agents, while still providing "full-stack visibility" into your cloud assets. Achieving full-stack visibility has become even more crucial, because what you can't see carries the risk of unforeseen and unmanageable risks.

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

Full-stack visibility into four layers:

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

According to Gartner, "Through 2025, more than 99% of cloud breaches will have a root cause of customer misconfigurations or mistakes."[1] Gaining visibility into cloud configurations is therefore crucial in order to maintain a secure cloud environment.

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

1

Cloud Infrastructure Level

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

2

Operating System Level

Common issues like remote code execution vulnerabilities (e.g. Microsoft Windows SMB Vulnerability) 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 you applied all required patches?

3

Application Level

This layer is where the vast majority of vulnerabilities reside. One example 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 all data inventory and where it is housed. Clear visibility is critical in order to determine where the organization's crown jewels are, and which servers include sensitive data such as PII or payment information.

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

Security Risks of Sprawling Cloud Deployments

One of the first issues that arise is **determining the administration of cloud resources; i.e. "Who is in charge around here?"** The traditional network model no longer exists, and cloud adoption has commonly created some friction among security teams and other departments in the organization. Defining roles and responsibilities within the cloud between DevOps, sys admins, outsourced staff, and any subsidiary organizations may create not only dysfunction, but also security weaknesses from rogue asset deployments, forgotten assets, and misconfigured or forgotten user accounts. DevOps teams should be able to innovate without waiting for security tools to be integrated with assets deployed in the cloud!

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 solutions don't provide complete visibility. On average we have seen that less than 50% of all cloud assets are covered by all the security solutions an organization leverages. As a result, they cannot reliably answer basic questions such as:

- ✓ "Do I have servers vulnerable to XYZ?"
- ✓ "How many servers running ABC do I have?"
- ✓ "Do I have sensitive data stored insecurely?"
- ✓ "How many versions of this database exist?"

The cloud layers and a breakdown of their specific security concerns

CLOUD SECURITY PLATFORM CAPABILITIES	CWPP	CSPM	EXAMPLE
Cloud Infrastructure	Defines who can access the machine (its IAM 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 which is mistakenly connected directly to an external network.
Operating System	Manages, operates, and executes processes.	Into inventory and 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 operating system services, such as PrintNightmare.
Application	Applications installed on a machine, such as web servers, CRMs, databases.	Into 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 cryptomining scripts installed on a machine.
Data Stack	The data that resides on top of the apps, 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 methods of visibility into the cloud include:

- CWPPs (agent-based)
- CWPPs (network scanner-based)
- Cloud security posture management solutions (CSPMs)

Each method has their distinct pros and cons. The chart to the right breaks down each type of solution and its capabilities.

CLOUD SECURITY PLATFORM CAPABILITIES	CWPP	CSPM	orca security
Risk to scanned assets	🟠 Medium	🟢 None	🟢 None
Operating cost	🔴 High	🟢 None	🟢 None
Security Visibility (Depth)	🟠 Medium	🔴 Very Low	🟢 High
Security Visiblity (Breadth)	🔴 Low	🟠 Medium	🟢 High
Workload OS Support	🟠 Medium	🔴 N/A	🟢 High
Can be circumvented by malware	🔴 Yes	🔴 N/A	🟢 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 (can't scan workloads)	🟢 Yes
Cloud Level Misconfiguration Detection	🔴 No	🟢 Yes	🟢 Yes
Physical System Support	🟢 Yes	🔴 No	🔴 No
Scan stopped machines	🔴 No	🔴 No	🟢 Yes

1. Agent-based Solutions

Agent-based solutions require software agents installed for each asset to be monitored. Qualys Cloud, Rapid7 Insight, and Tenable.io are some of the more popular agent-based solutions available.

How they work

Agent-based solutions require agents to be installed for each asset, either manually or using a tool. 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 software updates from time to time.

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

PROS

- Delivers in-depth visibility into issues within the OS, applications, and data status by looking into files, processes, and registry data.
- Able to detect malware and vulnerabilities on the host.
- Provides ongoing 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.
- Incompatible with some assets such as native cloud storage, cloud databases, and certain endpoint types.
- Can't detect cloud-level misconfigurations. Agents cover three of the four cloud layers — OS, applications, and data — but they don't scan the cloud infrastructure.

2A. Network Scanners - Unauthenticated

Similar to agent-based solutions, 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 fall into two basic types; authenticated and unauthenticated.

How they work

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

Maintenance

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

PROS

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

CONS

- The scanner can inadvertently create outages on the services when trying to connect to a host to determine if vulnerabilities exist. There is a fine balance between the detection level and a tolerable risk level.
- 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 explicitly 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 the large number of networks within the cloud environment.

2B. Network Scanners - Authenticated

Similar to agent-based solutions, network scanning tools attempt to identify possible vulnerabilities on the host. Products in this category include solutions from Qualys, Rapid7, and Tenable.

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, apps, 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 Solutions (CSPMs)

How they work

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

Maintenance

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

CSPMs don't penetrate the layers above the cloud I/S, failing to provide visibility to OS and application level vulnerabilities and breaches.

PROS

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

CONS

- Limited security visibility depth within each asset, covering the lowest level of the stack. It cannot provide visibility into the OS, apps or data layers.
- Doesn't use workload security data to help prioritize the criticality of cloud 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 bulletproof security. One or more assets on one of the four layers will almost certainly lack full-stack visibility into cloud, OS, applications, and data. It's also highly likely that the assets lacking visibility are those 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 eliminate some of the deficiencies, but the more integration that's required means that more time, management, and manpower will also be needed.

The Orca Agentless Cloud Security Platform

Orca delivers a single agentless SaaS-based platform for workload and data protection, cloud security posture management, vulnerability management, and compliance management. In response to the shortcomings of agents and network scanners, Orca developed a revolutionary new technology called SideScanning™ that dives deep into the workload without the constraints and operational costs of these legacy tools. So instead of interfering with your cloud environment and causing more problems, we collect data (with read-only access) directly from the workload's runtime block storage as well as from the cloud provider's API as a CSPM. As a result, we don't have to run any code or send a single packet in your environment. This approach has allowed Orca to disrupt the cloud security industry — and in fact, turn it on its head.

How it works

After a quick, 30-minute deployment process and initial scan, Orca surfaces the most critical security risks that threat actors use or exploit.

Issues like vulnerabilities in operating systems and applications — including the components that make up applications, namely packages and libraries. Orca detects misconfigurations and malware on machines that have already been compromised and those 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 cloud keys left behind that provide root access due to poor security hygiene — or secure shell keys that facilitate access to the entire cloud environment.

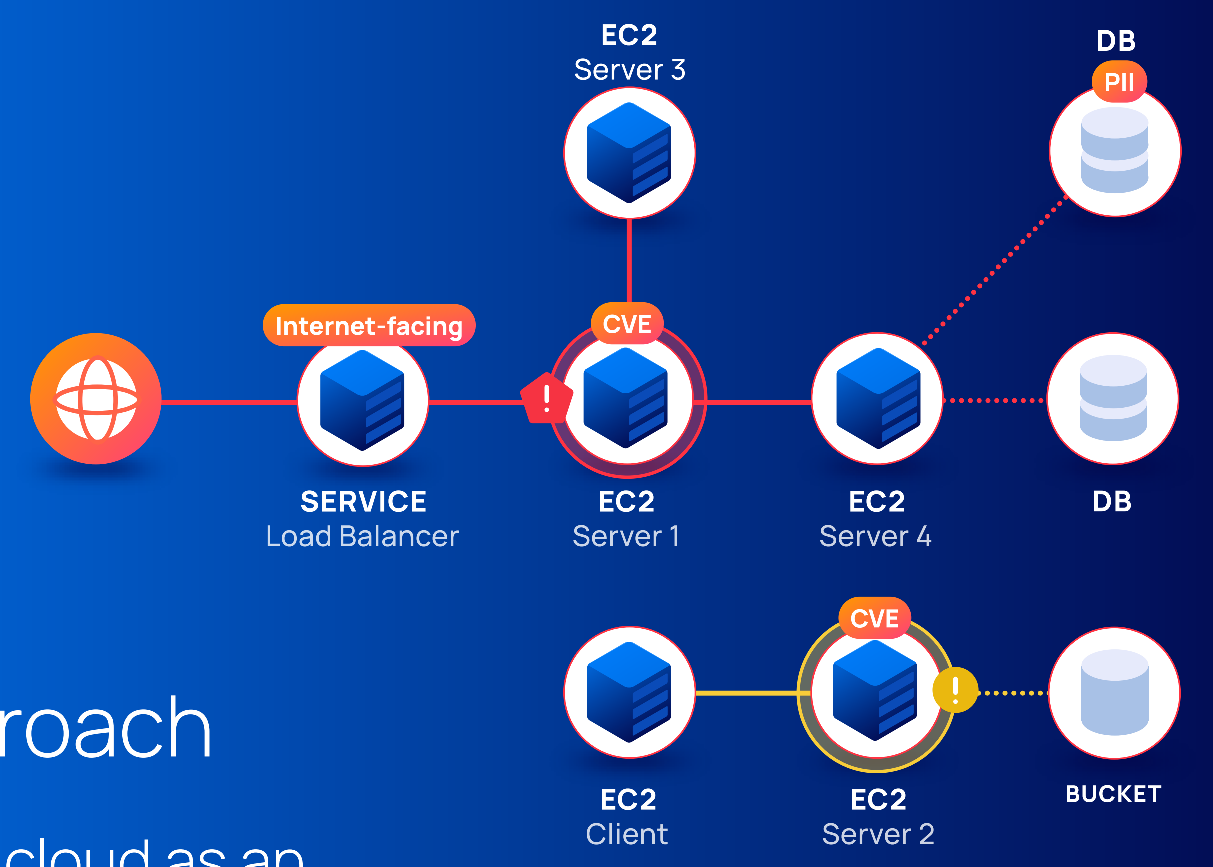
Intelligence Powered by Context

Combining the intelligence from the workload (workload plane) with the cloud metadata (control plane) enables Orca to obtain complete visibility into your entire cloud estate, as well as understand the connection between different assets. With this visibility, Orca builds the context necessary to truly understand your cloud 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 cloud (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 lots 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 time assessing the priority of each issue.

We see risk as much more than just the severity of the underlying security issue — 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).

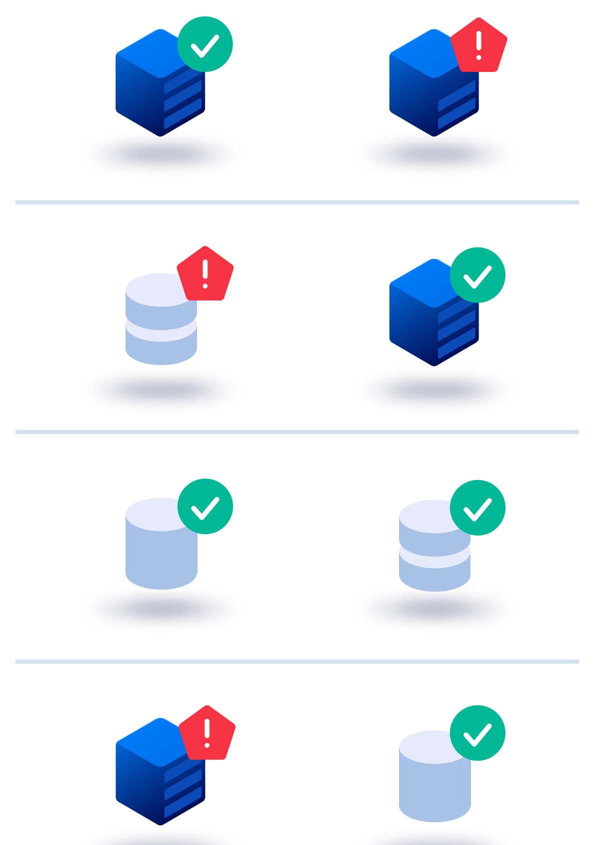
This results in effective prioritization of critical alerts, dramatically reducing the time needed to sift through large volumes of alerts and determining which alerts are truly critical and which are false positives. In fact, Orca reduces alerts by 99.9% compared to other solutions.



Orca's Approach

Orca sees your cloud as an interconnected web of assets.

VS.



Other Solutions

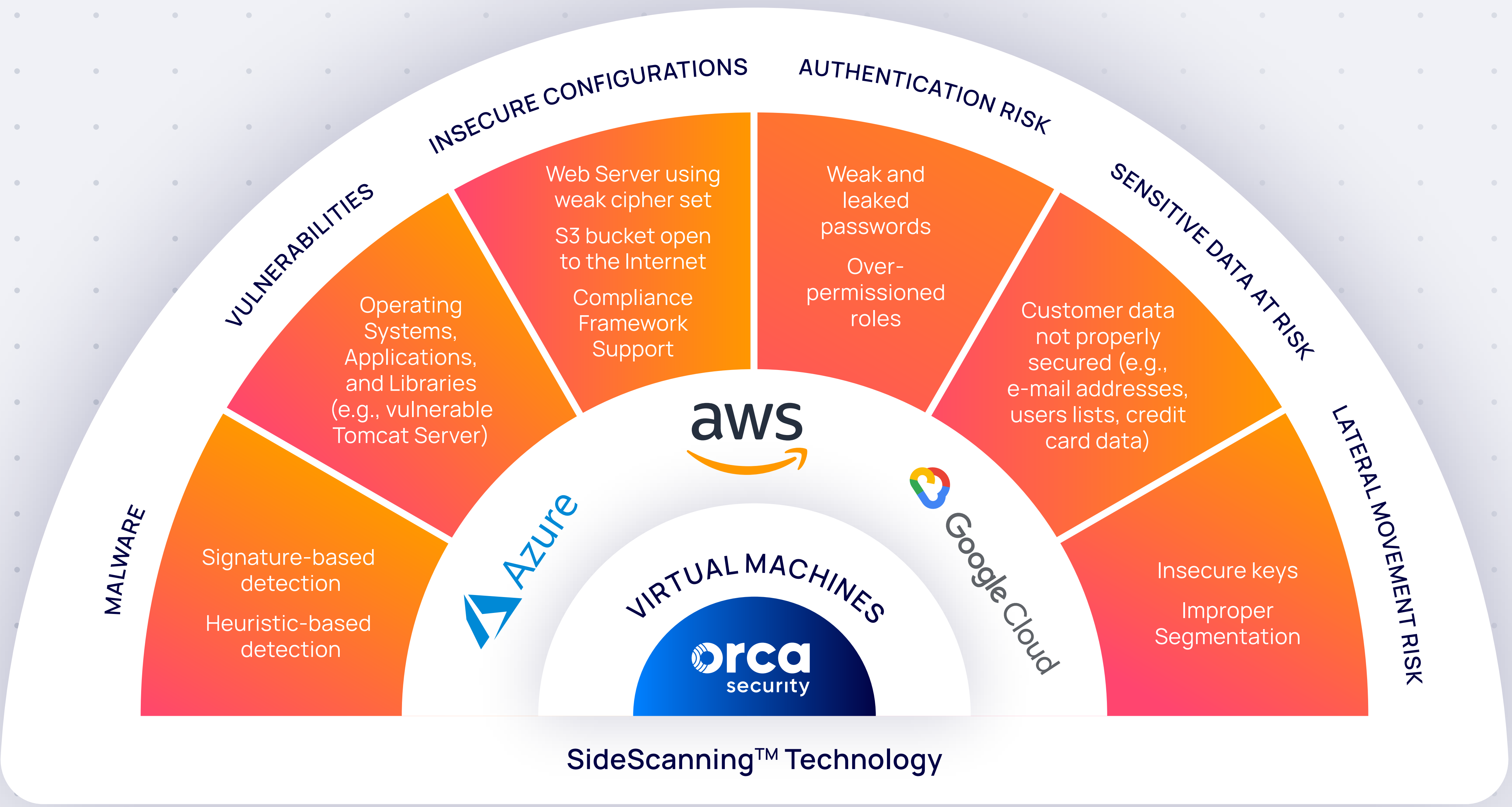
The other vendors see your cloud as a simple list of assets.

Multiple Tools in One Platform

Orca reduces operational costs and improves effectiveness by providing a single platform with the core capabilities of CSPM, CWPP, vulnerability management, and compliance solutions. This allows security teams to get a complete picture of the security and compliance issues across your 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 cloud security data, leaving you with more time to devote to higher-value activities.

Major Risks Covered


MALWARE
Signature-based detection
Heuristic-based detection
VULNERABILITIES
Operating Systems, Applications, and Libraries (e.g., vulnerable Tomcat Server)
INSECURE CONFIGURATIONS
Web Server using weak cipher set
S3 bucket open to the Internet
Compliance Framework Support
AUTHENTICATION RISK
Weak and leaked passwords
Over-permissioned roles
SENSITIVE DATA AT RISK
Customer data not properly secured (e.g., e-mail addresses, users lists, credit card data)
LATERAL MOVEMENT RISK
Insecure keys
Improper Segmentation
Azure
aws
Google Cloud
VIRTUAL MACHINES
orca security
SideScanning™ Technology

"We plan to replace several one-off solutions with Orca because Orca does much more than just vulnerability scanning. It looks for data loss prevention. It does virus scanning. It performs an inventory. Orca does it all, while saving us both time and money."

Thomas Hill
CISO, Live Oak Bank

Read the full story at Orca.security/live-oak-bank-technology

Ease of Maintenance

Orca's platform is deployed in a matter of minutes to get full-stack visibility into the security posture of all assets in the entire cloud footprint. There is no need to constantly monitor or integrate new systems. As it leverages read-only integration, there is absolutely no risk involved. Given that Orca detects every important security risk at every layer of your cloud estate, from the control layer to the workload layer to the data stack layer, it can replace multiple solutions — such as legacy vulnerability assessment tools, as well as CSPM and CWPP solutions — which reduces operational costs and improves ROI.

SideScanning provides full stack visibility to all of the assets.

PROS

- Full-stack visibility into all of your assets in minutes. As it doesn't rely on the OS, it can even scan paused, stopped and idle machines.
- Deep security visibility on vulnerable software, non-secure configurations, exploitation attempts, and compromised assets.
- Utilizes read-only access, so there is no performance or availability impact.
- Provides full-stack asset inventory for your entire cloud deployment. No gaps in coverage.
- 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 I/S level covers all assets, no matter how many exist.
- Since it doesn't rely on the scanned machine, Orca's side scanning solution can detect rootkits and malware which can circumvent security agents.

CONS

- Does not currently cover IoT devices.
- Does not support bare metal environments.

Conclusion

While each of the conventional cloud security solutions has its strengths, when it comes to cloud visibility, it's clear that no matter which one is implemented, there will always be something missing in cloud coverage. Even when deploying a combination of agents, 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 cloud assets.

For more information on the Orca Security Platform

Contact: info@orca.security

"Orca Security gives us 'X-ray and thermal vision' across our entire cloud infrastructure. It gives us that one alert that pinpoints what we need to pay attention to. That's huge because it lets us run lean-and-mean, with everyone totally focused on where they need to be."

Michael Meyer
Chief Risk and Innovation Officer,
MRS BPO

orca security

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.

Orca Security is trusted by global innovators, including Databricks, Lemonade, Gannett, and Robinhood. Connect your first cloud 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