orca security

Evaluating Agentless Cloud Security Solutions?

7 Questions You Must Ask Your Cloud Security Vendor

Here are the 7 questions you MUST ask your cloud security vendor

Vendor claims can make it difficult for defenders to separate fact from fiction. Orca Security is the cloud security innovation leader, is the inventor of SideScanning™, and has the patent application dates to prove it.

Use these questions to make an informed decision and make sure you include the relevant questions in any public cloud security vendor RFP.

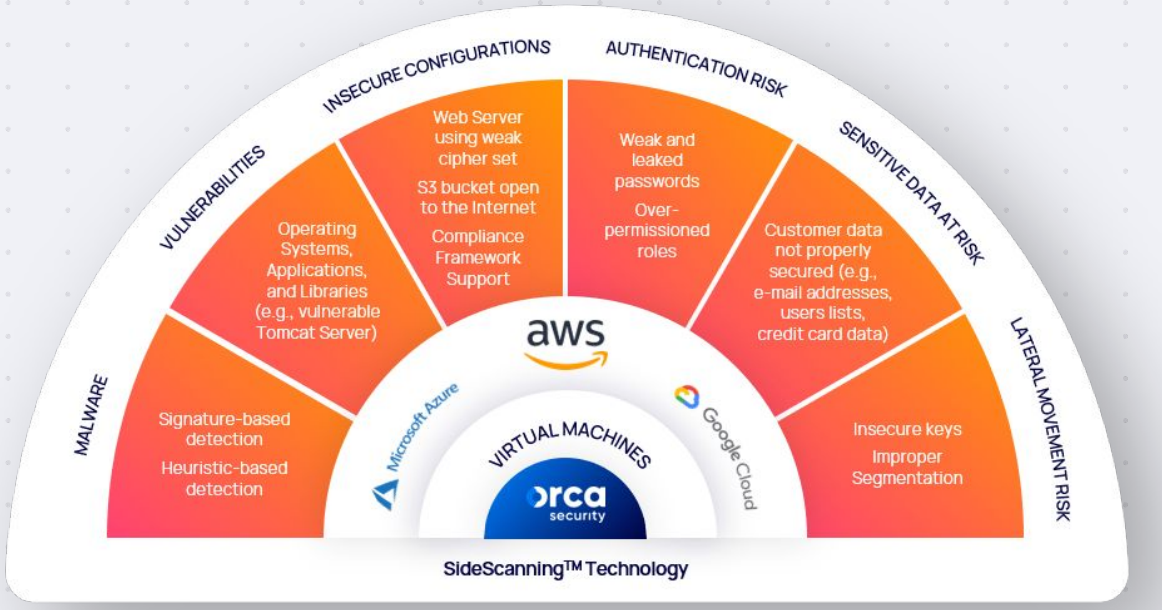
1

What types of cloud security risks are you able to detect within my environment?

Vendors that lack critical capabilities such as malware detection or the ability to identify sensitive data at risk can weaken your overall security posture and make it difficult to meet compliance mandates such as PCI-DSS, HIPAA, and GDPR.

As shown in the diagram, Orca detects the following types of risk:

- Malware including both signature and heuristic-based detection
- Vulnerabilities in operating systems, applications, and libraries
- Insecure cloud configurations
- Authentication risk such as weak and leaked passwords, as well as over-permissioned roles
- Sensitive data at risk including PII
- Lateral movement risk due to insecure keys and improper segmentation



"We needed a solution that could provide complete visibility into our cloud estate while also scanning for malware, identifying misconfigurations, and protecting PII."

Shahar Maor
CISO
Fiverr

fiverr.

2

How does your solution ease our compliance efforts?

As noted previously, having a complete solution that covers malware scanning and sensitive data at risk is critical to meeting compliance mandates.

Also, ask your vendor which compliance frameworks they support and how they make it easy to provide evidence to auditors.

As for Orca, we empower your security team to support continuous compliance with all key frameworks, including PCI-DSS, SOC 2, PSD2, GDPR, NIST-800, and HIPAA. Orca supports a wide range of CIS control benchmarks such as Apache CIS, AWS CIS, Azure CIS, Docker CIS, GCP CIS, Linux CIS, Windows CIS, and more.

In addition to out-of-the-box compliance templates, Orca supports customization and automation via Orca's security context framework which includes auto-ticketing to Jira or ServiceNow for those repetitive or high-criticality cloud compliance issues.

With Orca, you can meet data privacy mandates such as PCI-DSS, GDPR, and HIPAA by showing regulators evidence of your ability to identify and protect sensitive data like PII. The Orca platform uniquely recognizes where sensitive data such as PII is located across your cloud estate and alerts you to all potential exploitation paths.

"Orca has helped reduce my audit effort; for example, I can run reports that show we maintain least privilege controls and that we use multi-factor authentication. Orca is great at detecting potential exposure of credit card data, email addresses, and social security numbers or other national IDs. These are priority issues that we can quickly remediate."

Jonathan Jaffe
CISO
Lemonade

Lemonade

3

Are there analyst reports, awards, or customer reviews that further validate the maturity and trustworthiness of your solution?

Analyst Research Reports

- 451 Research Report on Orca Security's Light, Agentless Approach to Cloud Security
- A 2021 Gartner Cool Vendor for Cloud Security Posture Management
- TAG Cyber Vendor Landscape and TCO Analysis: A Comparison of Pre-Cloud Tooling, CSPM, CWPP, and Orca Security's Next-Gen Cloud Security Platform

Orca has dozens of satisfied and referenceable customers and public reviews:

- Detailed Orca Case Studies
- Orca G2 Reviews
- Orca Gartner Peer Insights Reviews
- Orca Capterra Reviews

"Orca's combination of SaaS delivery, SideScanning technology, and access to cloud configuration APIs provides security visibility and context info different aspects of cloud security with less friction than agent-based approaches."

Fernando Montenegro
Principal Analyst Information Security
451 Research

4

What certifications and competencies do you have to validate the security of your solution?

Orca Security has the following third-party certifications and validations:

- ISO 27001
- ISO 27017
- ISO 27018
- SOC 2 Type 2
- AWS Security Competency

Orca Security is one of only nine companies in the cloud vulnerability and configuration analysis category to achieve the AWS Security Competency.

This differentiates Orca Security as an AWS Partner Network (APN) member that provides specialized software designed to help enterprises adopt, develop and deploy complex security projects on AWS. To receive this designation, APN Partners must show that multiple customers have validated their technology for the specific competency, possess deep AWS expertise with a well architected infrastructure, and deliver solutions seamlessly on AWS.

5

How do you prioritize alerts/issues? What reasoning and details do you provide along with each alert/issue?

A few things to keep in mind here. Is the vendor able to clearly articulate how they prioritize alerts? Does the vendor's priority levels look consistent across different types of issues/alerts? Does the vendor provide and clear rationale and explanation for why an alert is being categorized the way it is?

Alerts in Orca are graded according to the risk level they pose to your organization. There are four levels of risk, highlighted from lowest (informational) to highest (compromised).

INFORMATIONAL [SCORE 4]

Alerts with no clear attack vector and pose minimal risk to the organization, so are thus deemed informational.

HAZARDOUS [SCORE 3]

Alerts with no known exploit or not reachable from the outside but still lessen your security posture.

IMMINENT COMPROMISE [SCORE 2]

Alerts with a high probability that the machine will be compromised based on the findings and a viable external to internal attack vendor.

COMPROMISED [SCORE 1]

Alerts when malicious code or activity is existing on the asset.

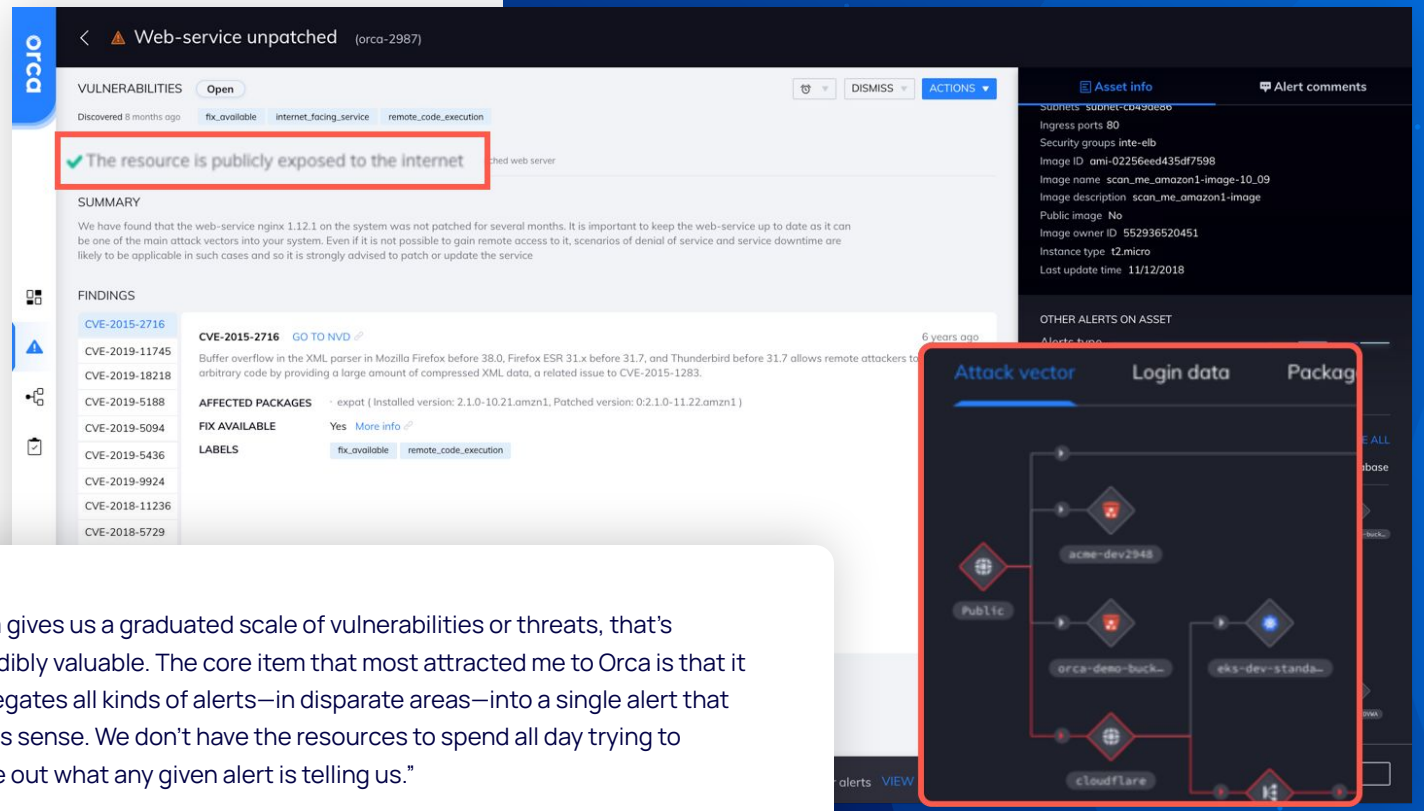
5

Alert Scoring can be upgraded or downgraded by taking multiple factors into consideration. Some examples are:

- Whether the asset is Internet-facing or not (Orca builds a context map to understand the topology, even if the asset is behind a proxy, load balancer, etc.)
- Vulnerability correlation to network services
- The publication date of CVE
- Fix availability per package/CVE by the vendor
- IOC – Indicator of Compromise (authentication logs, etc..)
- Exploit availability per CVE
- CVSS score baseline
- Potential damage like remote code execution or denial of service
- Trending/High-Profile CVE (security blogs, threat intelligence, Twitter chatter, etc…)
- Risky configuration (both the cloud control plane and workload risky configuration)
- Asset state (running /shut down)

5

In the screenshot to the right, Orca is showing an unpatched web service vulnerability. As explained in the alert itself, its severity is justified by the fact that the resource is exposed to the Internet. The visual attack map helps you understand how a would-be attacker could access this resource from the Internet.



Orca is the only vendor that effectively prioritizes alerts by taking a holistic approach to risk by combining workload data (vulnerabilities, misconfigurations, malware, file integrity monitoring), threat intelligence, and environmental context (accessibility and potential business impact).

"Orca gives us a graduated scale of vulnerabilities or threats, that's incredibly valuable. The core item that most attracted me to Orca is that it aggregates all kinds of alerts—in disparate areas—into a single alert that makes sense. We don't have the resources to spend all day trying to figure out what any given alert is telling us."

Michael Myer
Chief Security and Innovation Officer
MRS BPO

MRS
INNOVATIVE SOLUTIONS. REAL RESULTS.

orca security

6

How do you shorten time to resolution/remediation?

Alert prioritization is critical

Solutions that separate the 1% of alerts that matter help you focus your efforts on where they need to be. Equally important is that the solution give you a clear path forward to resolution.

FOR EXAMPLE:

- Can the vendor's solution not just detect a rogue SSH key in a workload, but also tell you what else in your environment those keys provide access to?
- Can the solution not only find malware but also tell you if the machine that they found it on is accessible?
- How will the vendor's solution guide you in containing the damage?
- Can the solution not only detect cloud keys that a developer has embedded in a test script but also tell if those keys are for accounts that you control?
    - And if so, for what users?
    - Or is it something that someone spun up on a credit card to try and test something?

6

The fact is you'll need answers to the previous questions to go back and find the root cause and fix these problems today as well as reducing the chances of them happening tomorrow. At Orca, we help you understand the magnitude of the issue and how to ultimately solve the problem. Orca provides recommendations for corrective actions so security teams can expertly harden cloud environments and strengthen their security posture.

Orca not only provides the information to remediate the issue, but also gets it into the hands of the team member(s) that can actually fix the problem. Orca then closes the loop by providing visibility into remediations, notifying the IT operations team as issues are resolved so they can track their successes and turn their attention to other tasks.

Orca's integration with Azure Sentinel Security Center and ServiceNow makes the solution far more valuable for BeyondTrust. It uses Security Center like a SIEM, so Orca's findings pour right into Azure Sentinel Security Center. Orca Security can kick off a ticket in ServiceNow if an investigation or remediation is needed.

"We stood up integrations with Azure Sentinel Security Center and ServiceNow in less than a week, and it works flawlessly. One dashboard chart tells me time-to-triage from the moment Orca detects something. Our average time-to-resolution has been cut in half for anything critical. Once a ticket is closed, and Orca doesn't see the issue anymore, we have a closed-loop, which is important for our governance team and the people who must ensure we meet our SLAs."

Morey Haber
Chief Technology Officer,
Chief Information Security Officer
Beyond Trust

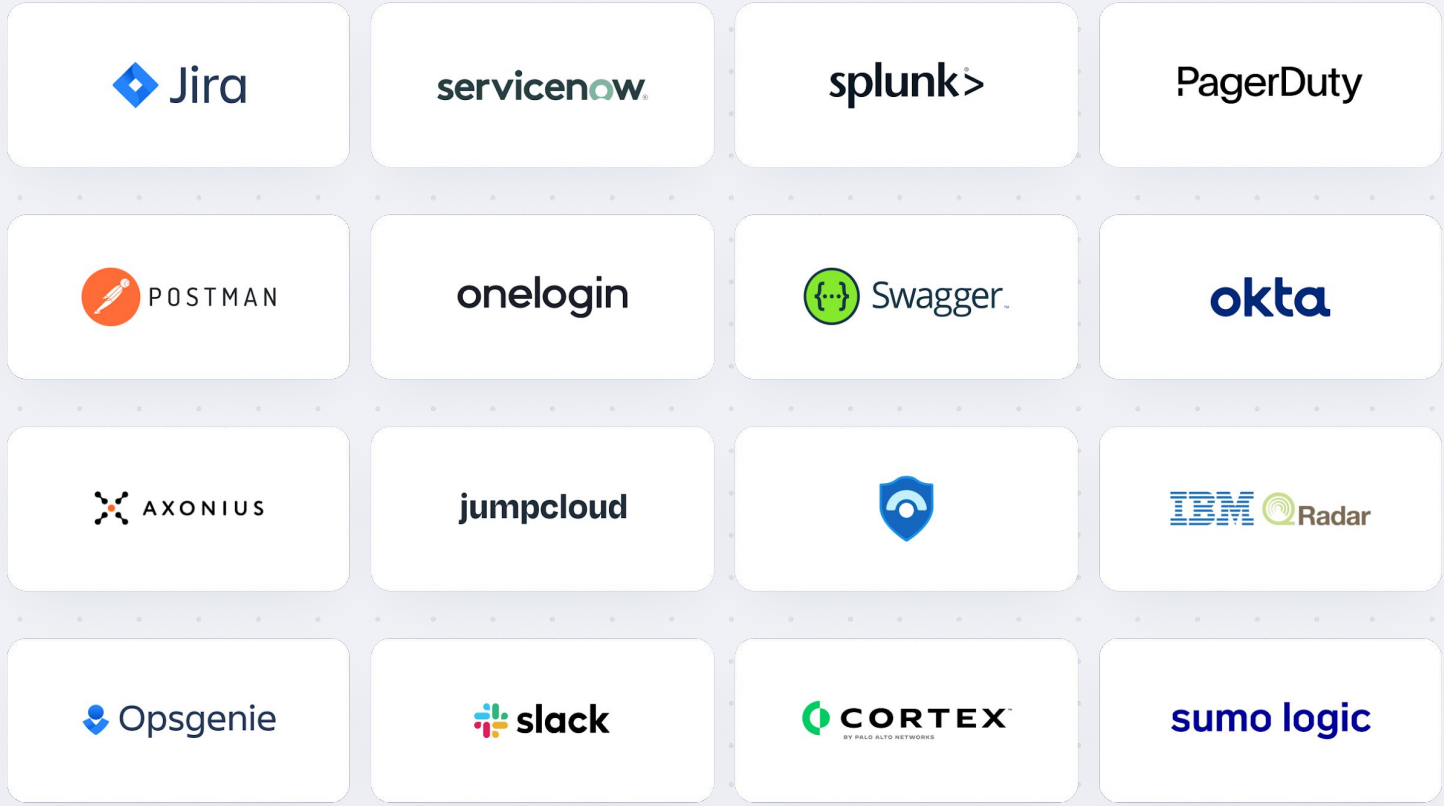
BeyondTrust

orca security

7

What integrations do you have today and what is the maturity of those integrations?

The cloud is about openness, and Orca is cloud-native in that regard. This means that authorized technology partners and customers can retrieve data or invoke operations via our public API. The same API that powers the Orca dashboard is open to you. Orca swims nicely with others as shown by our ever-expanding ecosystem of technology partners.

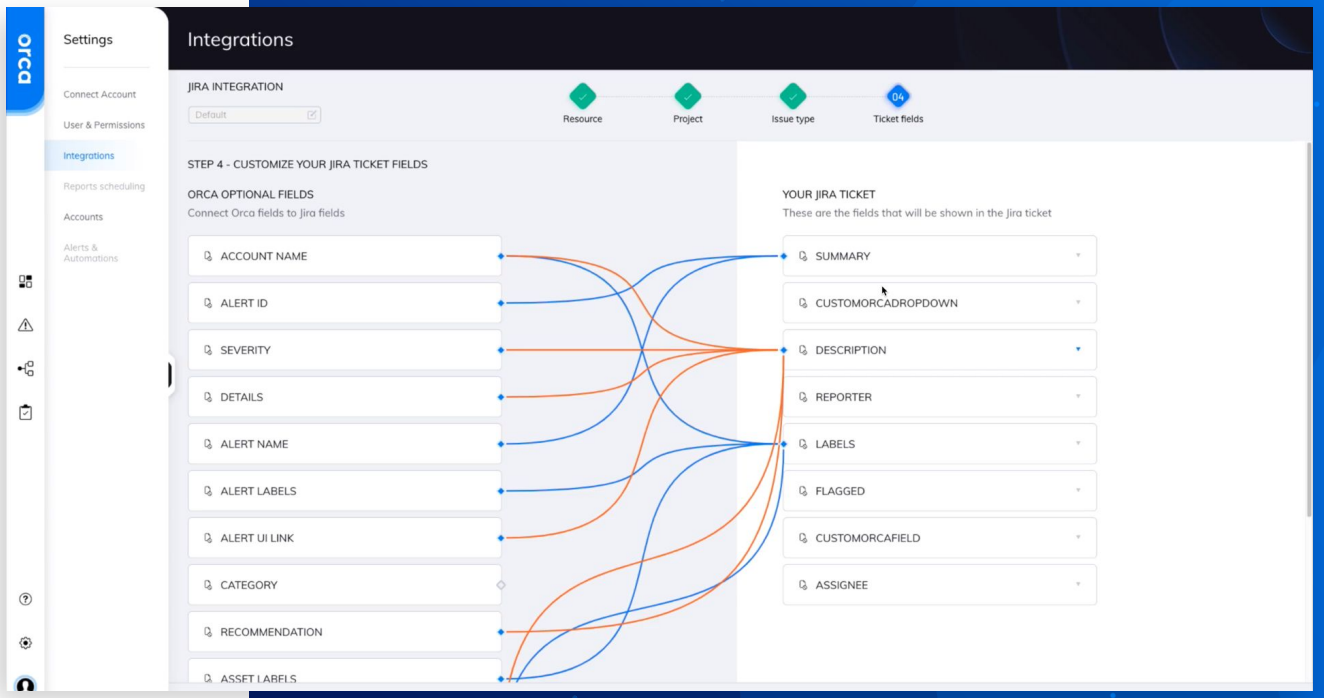


7

But just as important as the number of integrations is the quality and depth. As just one example, Orca has bi-directional sync with Jira that allows our customers to kick-off automated workflows that:

- Include the precise path to remediation
- Confirms the issue has been resolved
- Maintains evidence for auditors

The flexible Orca-Jira configuration interface can even support custom workflows.



"Knowing the tasks and associated risks at any moment, we can prioritize what we send to DevOps so they don't get overwhelmed. To assign the work, we simply click the 'send-to-Jira' button. If we get audited, we can show, 'This is our pipeline, this is our work plan.' It's all in Jira and everything has an audit trail. It just becomes very simple to demonstrate patching and compliance."

Nir Rothenberg
Chief Information Security Officer
Rapyd

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 or sidecars.

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 https://orca.security