

aws marketplace

Orca Security

Reviews, tips, and advice from real users



Powered by  PeerSpot



Contents

- Product Recap..... 3 - 4
- Valuable Features..... 5 - 10
- Other Solutions Considered..... 11 - 13
- ROI..... 14 - 16
- Use Case..... 17 - 22
- Setup..... 23 - 25
- Customer Service and Support..... 26 - 28
- Other Advice..... 29 - 33
- Trends..... 34 - 35
- About PeerSpot..... 36 - 37

Product Recap



Orca Security

Orca Security Recap

Orca Security provides comprehensive security management with agentless visibility and SideScanning technology, ensuring efficient threat detection without performance impact.

Orca Security offers agentless visibility across multi-cloud environments, streamlining security management with features like SideScanning technology and centralized security tools. It focuses on automation, vulnerability management, and compliance checks, enhancing a company's security posture with real-time alerts and integrated threat detection. Its intuitive interface prioritizes critical issues, making it suitable for managing DevSecOps processes efficiently.

What are the key features of Orca Security?

- **Agentless Visibility:** Gain comprehensive insights into cloud environments without deploying agents.
- **SideScanning Technology:** Detect threats and vulnerabilities efficiently across platforms.
- **Comprehensive Security Management:** Centralizes security across AWS, GCP, and Azure with minimal setup effort.
- **CIEM Feature:** Enhances security posture with integrated identity and access management.
- **Real-Time Alerts:** Provide immediate awareness of security threats and vulnerabilities.
- **Automation and Compliance:** Streamline processes with automated vulnerability management and compliance checks.

What benefits and ROI should companies look for in Orca Security?

- **Centralized Management:** Simplifies security operations by consolidating tools across cloud environments.
- **Improved Security Posture:** Reduces alerts and manages threats effectively with detailed insights.
- **Efficient Threat Detection:** Enhances response capabilities with integrated threat detection and real-time alerts.
- **Easy Deployment and Setup:** Facilitates quick implementation without complex configurations.
- **Enhanced Integration:** Supports seamless integration with existing security frameworks and processes.

Companies in industries such as finance, healthcare, and technology leverage Orca Security for cloud security posture management, ensuring compliance with standards and securing applications and databases. Its agentless approach provides comprehensive visibility across AWS, GCP, and Azure, enhancing risk assessment and vulnerability management without impacting asset performance.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Orca Security integration was one of the easiest we have done because it is cloud-native and agentless.”



Verified user

Soc Analyst at a tech consulting company with 11-50 employees

- ✓ “Orca Security saves resources because it provides the actual output on the screen with the package path.”



Verified user

Assistant Manager at a manufacturing company with 10,001+ employees

- ✓ “Orca Security is easier to use than other alternatives; you need a little skill to dominate Orca Security compared to other options and Orca Security is more user-friendly and in this case is more enjoyable.”



Ricardo Escriba Robles

Co E Cloud Security at Banco de Crédito BCP

- ✓ “Orca Security is the best one for me because it delivers all the things that I need and more.”



Fabricio Galdino

Cyber Security Analyst Ii at Grupo PRIMO

- ✓ “In our opinion, Orca Sensor is the best solution available at the moment, and it significantly affects the visibility and protection of environments.”



Evgeny Shulga

CTO /Director at OPLIUM

- ✓ “Overall, I think Orca Security is the leader because of the strategic features I mentioned.”



Verified user

Cybersecurity Recruitment Specialist at a tech services company with 51-200 employees

- ✓ “I appreciate Orca Security because I can see CSPM, KSPM, and DSPM, and it works with major security frameworks such as NIST and CIS, allowing me to see comprehensive insights on my cloud environment, with CI/CD integration and shift-left configuration that helps me improve cloud maturity and DevSecOps maturity as a complete CNAPP platform with the most capabilities to work with cloud security.”



Kaue Ribeiro

Cybersecurity Architect Lead at a consultancy with 11-50 employees

What users had to say about valuable features:

“I find Orca’s secret scanning and 'Shift Left' capabilities to be most valuable. The platform integrates directly into our GitHub and Azure DevOps pipelines, which allows us to automatically analyze pull requests for hardcoded passwords, API keys, and other sensitive credentials..”

RicardoEscriba Robles

Co E Cloud Security at Banco de Crédito BCP

[Read full review](#) 

“The vision related to security frameworks is very valuable for us, and we use that to be compliant with standards such as PCI DSS. The way to create dashboards is very useful for us as well.

It is easy for us to have one place to check things, and when we need to create some report for our teams or for another team, we use these compliance visuals to see what is compliant and what is not compliant..”

Rodrigo Americo

Security Engineer at a computer software company with 501-1,000 employees

[Read full review](#) 

“Orca Security is a really strong product because it has a lot of different differentiators. Orca Security is based on agentless side scanning, so it has the ability to scan cloud workloads including virtual machines, containers, and serverless infrastructure all without installing any software or agents. This results in zero performance impact on production, which I think is the most important thing in the market share or in an eventual Gartner Quadrant.

Orca Security helps in preventing risks and attacks across the application lifecycles by scanning not only the apps in production, but also the apps or microservices in development. This provides complete visibility to your infrastructure..”

Verified user

[Read full review](#) 

Cybersecurity Recruitment Specialist at a tech services company with 51-200 employees

“One of Orca Security's main features is its agentless architecture, enabling it to conduct cloud security gap analysis and vulnerability scans without installing agents. The tool offers visibility into attack paths and predicts potential impacts if an exploit occurs. Furthermore, it includes identity and risk access analysis, CIEM, and Kubernetes cluster scanning. The product integrates well with CI/CD pipelines for identifying IaC misconfigurations. I appreciate its side scanning and workload visibility, which is valuable for analysts involved in security posture management and audit evidence collection..”

Verified user

[Read full review](#) 

Soc Analyst at a tech consulting company with 11-50 employees

“The best feature is Orca Side-Scanning. Because of this feature, the platform does not need to use agents for the detection of virtual machines, containers, and hosts. It can connect via a cloud-native API and perform out-of-band scanning using read-only access. Orca Side-Scanning has made things both easier and faster for security teams and for the people who have to act on findings. This platform is very useful for the maintenance of vulnerability in cloud environments, with the impact on the security team's workflow being a much faster time-to-value.

“The Attack Path feature is a great option for the capabilities of Orca Security's strengths because it models network exposure, permissions, vulnerabilities, and trust relationships. This feature helps security teams think like attackers and identify high-impact risks..”

Marcus Cassilia

Cyber Security Consultant at ShieldSec

[Read full review](#) 

“What I love most about Orca Security is the easy integration with other tools. I really like it because it's very easy to integrate with other tools that are important for the company. It's already set up in the platform easily. I don't need to do unusual modifications or create a script. It's pretty easy to integrate these tools.

It is easy to prioritize risks using Orca Security because they have already been categorized. The severity of some risks is delivered from Orca Security, and I can set some kind of high-value asset designation. I can define what is a high-value asset or not. The attack paths also help me to understand the prioritization of the risks of these assets.

Orca Security has helped my company reduce the time it needs to address cloud security alerts and make it faster. When one critical risk or high risk is identified in my environment, I already receive notifications, even in email or in Teams, Slack, or any channel that is integrable to Orca Security. I receive a very fast notification to address the vulnerability and security issues to the teams..”

Fabricio Galdino

Cyber Security Analyst II at Grupo PRIMO

[Read full review](#) 

Other Solutions Considered

“In my opinion, Orca Security compares to other products and vendors on the market as something disruptive. I believe it can be very interesting at this moment..”

Evgeny Shulga

CTO /Director at OPLIUM

[Read full review](#) 

“We used the Prisma solution from Palo Alto in the past, and I believe we changed to Orca Security because of the price that Orca Security offered. However, that is not something that relates directly to me, so I am not certain about that..”

Rodrigo Americo

Security Engineer at a computer software company with 501-1,000 employees

[Read full review](#) 

“I tried similar solutions from Trend Micro. From Trend Micro, I also tried a new one that is called Wiz. Orca Security is the best one for me because it delivers all the things that I need and more..”

Fabricio Galdino

Cyber Security Analyst Ii at Grupo PRIMO

[Read full review](#) 

“Similar solutions to Orca Security are Prisma Cloud, Microsoft Defender for Cloud, Wiz, and Qualys. However, I think Prisma Cloud is the same as Orca Security, but Prisma Cloud is more expensive than Orca Security..”

RicardoEscriba Robles

[Read full review](#) 

Co E Cloud Security at Banco de Crédito BCP

“We had Wazuh or Falco OSS or Aqua Security which was very excellent. It had blocking and cloud content but ops overhead was very high. Orca Security is very low on that. We also use SentinelOne which had blocking and its own automation, but cloud context is very less. We used to write a lot of manual rules for that which used to take our engineer's time. These are the three tools which I previously worked with and I know there are a lot of other tools in the market. In my experience, Orca Security was a top one or top three tool..”

Verified user

[Read full review](#) 

Soc Analyst at a tech consulting company with 11-50 employees

“Regarding the extent to which Orca Security helps in preventing risks and attacks across application lifecycles, I think it is the same scenario because there are many CSPM tools available. We have Wiz, Orca Security, and Lacework. All CSPM tools do the same work by scanning the infrastructure and providing reports either through API or through sensors. Definitely, the risk is more important on the cloud misconfiguration side because they tell us about the misconfigurations. CSPM is not a vulnerability management tool. It is more on the cloud side where they provide misconfigurations related to that. After you have deployed something on your infrastructure or cloud infrastructure, once you put a CSPM in your infrastructure, it will tell you how effectively you can remove those misconfigurations. That is the edge that CSPM is giving..”

Verified user

Assistant Manager at a manufacturing company with 10,001+ employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I see the benefits of Orca Security immediately because you can see the issues right after deployment, and you can correct the critical issues, so the proof of value is immediate..”

Kaue Ribeiro

Cybersecurity Architect Lead at a consultancy with 11-50 employees

[Read full review](#) 

“Orca Security significantly improved our visibility from 30% to 100%, enabling better security posture improvements rather than just general cost savings..”

CHINTAN MEHTA

Cloud Security Automation Engineer at a financial services firm with 10,001+ employees

[Read full review](#) 

“The ROI or return on investment with Orca Security might be favorable. The TCO or Total Cost of Ownership is an important term. While the initial sticker price might be higher than point solutions, the total cost of ownership is much lower. This is because you do not need a team of five persons to install and update the agents in thousands of servers. The operational overhead is equal to zero..”

Verified user

[Read full review](#) 

Cybersecurity Recruitment Specialist at a tech services company with 51-200 employees

“When you're talking about return on investment, you have to consider the resources needed to implement, maintain, and support a tool. With Orca, we didn't need to deploy or upgrade anything, and we didn't need to understand anything about support because they already had great support. I think we're saving hundreds of thousands of dollars every year in staffing costs alone. The time-to-value was instant. .”

Verified user

[Read full review](#) 

CISO at a financial services firm with 51-200 employees

“We've seen a return on investment insofar as that can be measured for an essential tool. We're not planning on giving Orca up, but it all depends on the price of competitors like Wiz. If their price drops and it's significantly cheaper than Orca, it's easy to switch. Also, the time to value for Orca was immediate — 24 hours — so it's much better than other solutions. With Lacework, it took at least a month before we saw any value, and then the value was extremely low..”

Verified user

CISO at Lemonade Inc.

[Read full review](#) 

“This product has saved us tremendous amounts of time and money.

I would just say that you're doing yourself, your business, and your customers a disservice if you're not using Orca, or a tool like it, that provides a deep X-ray-like view into your environment to properly secure it.

We would not be in the cloud or have as much in the cloud without this tool. It's really a precursor to moving anything major into the cloud. In that regard, it's our future. Cloud is our future and without Orca carrying that future, we can't do the things that we want to do. It's very difficult for me to put a return on investment on it because it's so intertwined with everything that we do. We wouldn't be able to do the things that we do without it..”

Verified user

Chief Risk Officer at a financial services firm with 51-200 employees

[Read full review](#) 

Use Case

“Orca Security provides three main strategic advantages. First, there is 100% visibility because it does not require agents. It can see everything, even shadowing or abandoned servers that the security team did not know existed. The main responsibility is side scanning, which is the first technology by Orca Security. Second, there is context-aware risk prioritization. Instead of drowning security teams in a sea of maybe 10,000 alerts, Orca Security uses a graph-based engine. It understands that a vulnerability on a web-facing server with access to a database is much more dangerous than the same vulnerability on a test server with no internet access. Third, there is operational efficiency. It saves hundreds of hours for DevOps teams who no longer have to install, update, or troubleshoot security..”

RicardoEscriba Robles

Co E Cloud Security at Banco de Crédito BCP

[Read full review](#) 

“When discussing the main use case for Orca Security, I am referring to implementations for my clients. I participate in several CSPM implementations for my company, but I cannot comment much on the customers due to confidentiality rules. The projects that I participate in typically involve a cloud environment that is already in production, such as AWS, Azure Cloud, or GCP. We create a context of the environment and connect multiple accounts for scanning all assets and containers in the cloud accounts of customers. We perform onboarding and create initial maps of risks. Orca Security supports remediation with clear technical evidence, objective remediation recommendations, and monitoring of risk reduction over time..”

Marcus Cassilia

Cyber Security Consultant at ShieldSec

[Read full review](#) 

“I normally use Orca Security for AppSec, and one of the features that I use commonly is the application security. I love it because it's already covered in the same license, and I can get a good overview of all of my assets. I have a lot of accounts in cloud, and so it's sometimes hard to identify all activities or assets that have been used or not. Normally, some developers create some virtual machines and leave the VM on or don't remove it. Orca Security usually helps me to see these kinds of problems because I can see every asset in one platform.

I don't use the Cloud to Dev feature they mentioned, since I'm working with Orca Security directly.

I believe the feature referred to as Orca Sensor is cloud security detection. I use it frequently because it's very important. I really enjoy it because it's agentless. I don't need to install or build an agent in my assets in the cloud. Orca Security accomplished this safely and fast. It's pretty easy to identify security risks or security issues using Orca Security because it's totally agentless and I just need to connect my cloud environment. It's really good and pretty easy. They have one feature that I really like in this same vein; it's the news about security. For example, if a new vulnerability is found and it's not already published in a CVSS bug, Orca Security has new papers that already inform me, stating that I have this new issue and this asset has been affected by this new vulnerability, and it provides guidance on how I can fix it. I love it..”

Fabricio Galdino

Cyber Security Analyst II at Grupo PRIMO

[Read full review](#) 

“My use cases for Orca Security include working with the sales team and the pre-sales team to offer Orca Security in the Chilean market with an integrator or a partner of Orca Security. The real impact when the client or the potential client sees the POC is truly awesome because you can have 100% visibility since Orca Security provides full coverage across your entire cloud estate across AWS, Azure, and GCP within minutes, finding shadow assets that traditional tools like Cortex or Prisma from Palo Alto cannot detect.

Orca Security has other strategic features such as CNAPP or Cloud Network Application Protection Platform capabilities, including CSPM (Cloud Security Posture Management). You can detect misconfiguration and ensure compliance with frameworks like SOC 2, ISO 27001, or GDPR of the European Union. Another valuable feature is the Cloud Workload Protection Platform, where you can identify vulnerabilities such as CVEs, malware, and exposed secrets such as API keys or passwords inside your workloads during scanning. Another feature is Cloud Infrastructure Entitlement Management, where you can manage identities and permissions to enforce least privilege and find overprivileged accounts. Finally, there is Data Security Posture Management, where Orca Security can automatically discover and protect sensitive data such as PII and PHI to prevent data breaches..”

Verified user

[Read full review](#) 

Cybersecurity Recruitment Specialist at a tech services company with 51-200 employees

“I use Orca Security to analyze misconfiguration and to alert our SOC team when a misconfiguration occurs in our environment so that we can open an incident and solve it.

For example, we have one alert that triggers when a security group is created and a resource is created and exposed to the internet without an ACL attached on the resource and with the security group allowing any IP from the internet to access the resource.

We have created some custom alerts, and we are trying to create some automatic remediation using Orca Security. However, we need to open a ticket to support Orca Security to inform them that we need it, and it will go to the development team, which is not ideal for us as a customer.

I use the risk score related to our vulnerability management program in Orca Security to analyze and prioritize how to fix issues and what we need to fix first. Any resources that have a risk score more than seven are critical for us, and we prioritize the fix accordingly.

I use Orca Security in our public cloud environment.

Using Orca Security, I have visibility in our environment without depending on another team. I can connect our AWS accounts and our cloud accounts directly on the platform, allowing me to see and analyze our environment automatically.

We use AWS, Azure, and GCP.

I find that using the AI search feature is particularly valuable, as you do not need extensive knowledge of the platform to identify resources and define what you need to find..”

Rodrigo Americo

Security Engineer at a computer software company with 501-1,000 employees

[Read full review](#) 

“I use Orca Security to deploy in cloud infrastructures as a top-notch agentless SIEM and agentless cloud security platform. My use cases include cloud security, posture management, and detecting configuration misconfigurations across cloud environments. In AWS, which I use mostly for my work, it scans open S3 buckets, open ports, open IPs, and any open ports that are likely to be attacked or used as vulnerabilities. It also performs vulnerability management scans by running on VMs for CVEs, scanning containers, and providing serverless agents. It checks for outdated packages and OS level vulnerabilities without installing any agents. Having worked with other security platforms that have agents, I can confirm that one of Orca Security's main features is its agentless architecture.

Another significant use case is attack path analysis, which shows how an attacker could chain misconfigurations and vulnerabilities to reach the crown jewel of the environment. This is one of Orca Security's standout features. It visualizes the blast radius, demonstrating what the impact of a vulnerability would be. If an attacker exploits a vulnerability, it shows what may happen and what an attacker could do with all the vulnerabilities and misconfigurations combined.

Another feature is identity and risk access risk, which is CIEM that flags excessive permissions, unused roles, and privilege escalation paths within an IAM. Coming to container and Kubernetes security scans, it scans container images and Kubernetes clusters configurations for risk both before and after the deployment of those clusters. It has many other features as well. When we integrate it with CI/CD integration, it integrates with pipelines to catch Infrastructure as Code misconfigurations from Terraform or CloudFormation before deployment..”

Verified user

Soc Analyst at a tech consulting company with 11-50 employees

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“The initial deployment of Orca Security is easy; it is just plug-and-play on the cloud environment. When I deployed Orca Security for the first time, it took me around two days for cloud environments, no more..”

Kaue Ribeiro

[Read full review](#) 

Cybersecurity Architect Lead at a consultancy with 11-50 employees

“It was easy to install and set up everything. Setting up all the components, for example the sensors and the connection with our GCP, was straightforward and was assisted by someone on Orca Security's side..”

Rafael Bueno

[Read full review](#) 

Consultor de segurança da informação at a tech services company with 1,001-5,000 employees

“The deployment of Orca Security depends on the context because, for example, when I deploy in virtual machines, Kubernetes, or any resource, it is very easy. However, when I use other solutions by Orca Security, such as AppSec, it is more difficult..”

RicardoEscriba Robles

[Read full review](#) 

Co E Cloud Security at Banco de Crédito BCP

“The deployment is frictionless, and I think that feature is one of the most important.

I remember that the read-only connection is the deployment model we were using for Orca Security. Deployment is completely out of band, so we simply connect Orca Security through a read-only IAM role or service account at the cloud root level. You need root access..”

Verified user

[Read full review](#) 

Cybersecurity Recruitment Specialist at a tech services company with 51-200 employees

“The overall deployment is medium difficulty; it is not easy, but it is not complex either.

“How long deployment takes on average depends entirely on the amount of data and the questions we receive from the client's side. There are many factors to keep in mind, and the deployment timeline is influenced by various considerations..”

Evgeny Shulga

CTO /Director at OPLIUM

[Read full review](#) 

“Orca Security integration was one of the easiest we have done because it is cloud-native and agentless. I would give five out of five for the integration part. Deployment is that easy in Orca Security. That is one top-notch quality with Orca Security.

When we had this Orca Security deployment, it was very fast and took very minimal time compared to other agents. The primary strength is that it has attack path plus workload visibility which is very important. For teams wanting best time to value with minimal setup, Orca Security would be the choice.

The deployment method is very manual and we can use Ansible or Terraform to deploy Orca Security, which is one big advantage. Orca Sensor has very low deployment complexity and very high cloud context correlation..”

Verified user

Soc Analyst at a tech consulting company with 11-50 employees

[Read full review](#) 

Customer Service and Support

“In my case, I had technical support, and it is easy to contact the technical support. The quality of the support is good. If I were to rate the support on a scale from one to ten, I would give it an eight..”

Kaue Ribeiro

Cybersecurity Architect Lead at a consultancy with 11-50 employees

[Read full review](#) 

“I have had experiences where I needed to contact Orca support to address issues with alerts that remained active even after remediation. Based on my interactions, I would rate the support team a six out of ten..”

Srinath Swarna

Works at Ultraviolet Cyber

[Read full review](#) 

“Not so many people are required for the deployment of Orca Security; just one person can do it.

I have been in contact with technical support regarding Orca Security twice to solve some issues, but it wasn't an issue, just a wrong configuration that I made. I contacted them and they shared some documentation. After that, I could resolve it pretty well..”

Fabricio Galdino

Cyber Security Analyst II at Grupo PRIMO

[Read full review](#) 

“Technical support is very good, but customer support is very poor, in my opinion, because when I have a few problems, the customer support says your solution is bad or it is easier. However, the technical support is very good.

For example, the technical support has more experience in the solution, but customer support does not have more experience in the solution. Customer support does not know Orca Security in general. I think they have different skill sets..”

RicardoEscriba Robles

Co E Cloud Security at Banco de Crédito BCP

[Read full review](#) 

“The problem with the Orca Security technical support team and customer service team is that Orca Security is a medium company and I think they do not have a large team. If you have a lot of problems, you will receive an unprofessional service or unprofessional customer service because you do not have an entire team to respond to all of those kinds of problems.

I would rate the technical support team as a six..”

Verified user

[Read full review](#) 

Cybersecurity Recruitment Specialist at a tech services company with 51-200 employees

“I needed to contact support mainly for the custom tags issue I mentioned earlier. They are very clear and very fast with solutions. I could talk with engineers from Israel and India, and I also had a contact point in Brazil that helped me get responses as quickly as possible. I had a very positive experience with Orca Security support.

I would rate their support an eight out of ten. I had one or another problem that is on their roadmap to fix, but their answer was very fast. They communicated that certain features are planned but not currently available, or they might be ready for the next quarter. However, what they could help me with, they helped with as quickly as they could..”

Rafael Bueno

[Read full review](#) 

Consultor de segurança da informação at a tech services company with 1,001-5,000 employees

Other Advice

“I do not use Orca Security agentless exclusively for vulnerabilities. I appreciate Orca Security because it is a complete platform and its cost is very small compared with other vendors. I think the user interface of Orca Security is very intuitive, friendly, and easy to use. It takes me very little time to learn how to use Orca Security; I find it very easy to learn, and the documentation is online and intuitive. Overall, I would rate Orca Security at a nine out of ten..”

Kaue Ribeiro

Cybersecurity Architect Lead at a consultancy with 11-50 employees

[Read full review](#) 

“I have not utilized the Cloud to Dev feature. I do not know what level of subscription our company has taken for that feature. I think that is most suitably used in the development team. As per my knowledge, Cloud to Dev would be used for scanning Terraform or [CloudFormation](#) deployment config misconfigurations, which is what the cloud dev feature would be, but I have not used it because it is more of a developer thing. The overall review rating for Orca Security is seven out of ten..”

Verified user

Soc Analyst at a tech consulting company with 11-50 employees

[Read full review](#) 

“For my company, I don't use a huge workload. It's a small workload, around 90 workloads, but we have more. For this amount of workload, the price is high. When you have more workloads, the price is much better. I think it's not so expensive

when you have the right amount of workloads. It's more directed toward big companies.

I have tried to use Cloud Cost Optimization with Orca Security. We used it to reduce some costs by removing some unused assets. It really helped us, but I don't think that is the main focus of Orca Security. I use other tools to do FinOps in a better way.

I use a reseller that is a partner that helps me with Orca Security. I am just a client, but we have a company that sold Orca Security to us, and they are the bridge between my company and Orca Security company.

I would rate this product a 10 out of 10..”

Fabricio Galdino

Cyber Security Analyst II at Grupo PRIMO

[Read full review](#) 

“Orca Security typically delivers three major positive changes, in my opinion: a faster understanding of risks in cloud environments, better prioritization, and less noise. Orca Security enables collaboration between security and cloud teams for better troubleshooting and monitoring of the cloud environment. There is a faster time to visibility and results, along with a high reduction in security noise. I have a case of a customer who managed to significantly reduce the number of vulnerabilities in a team of development for web software and also in maintenance for virtual machines and containers for this environment.

“The deployment of Orca Security in my organization depends on which client is doing the implementation.

“The cloud providers my clients use most often with Orca Security are AWS and [GCP](#).

“I would suggest they test it and talk to Orca Security representatives because it will be a very positive experience for their company. I rate this product an eight out of ten..”

Marcus Cassilia
Cyber Security Consultant at ShieldSec

[Read full review](#) 

“Overall, my impressions of the risk detection and identification capabilities of Orca Security are that it has the capability to scan and show you all your infrastructure. If you have any kind of vulnerabilities, you can see them. It is very important to see all your infrastructure and all the possible ways to have vulnerabilities. Another important thing is if you need to scan all your workloads.

Overall, I think Orca Security is the leader because of the strategic features I mentioned. It is easy to analyze and detect breaches, anomalies, and misconfiguration. It is a tool that is designed to be very user-friendly.

The real value of Orca Security is not just finding vulnerabilities but reducing the noise so the security team can focus on the critical attack path. Orca Security is a really complete tool for cloud security. I think Orca Security reduces alert volume by focusing only on the one percent of risk that actually matters, which I refer to as the one percent rule. Orca Security filters the noise and reduces alert fatigue.

My advice for other organizations considering Orca Security is to remember that Orca Security is a great product, but the team should work on customer service. I gave this review an overall rating of eight..”

Verified user

Cybersecurity Recruitment Specialist at a tech services company with 51-200 employees

[Read full review](#) 

“Cloud security analyzes vulnerabilities or alerts by [IaaS](#) or PaaS because Orca Security analyzes these items very well. Side scanning is, in my opinion, the best tool by Orca Security. However, it is necessary to deploy the sensor agent in new tools, such as [Kubernetes](#), Lambda functions, and other services.

The sensor feature is good, but I prefer to use another alternative. For example, CSA by Cloud Security Alliance or by PCI or by CIS control is not optimized in Orca Security. I prefer to use another platform because these frameworks are more structured than Orca Security.

AppSec by Orca Security is the most interesting feature because it analyzes keys, passwords, and any methods for pull requests because it has integration with [GitHub](#), [Azure DevOps](#), and other platforms.

Orca Security continues to remodel the look and feel of the solution. In my opinion, it is very good. I would rate this review an eight out of ten..”

RicardoEscriba Robles

Co E Cloud Security at Banco de Crédito BCP

[Read full review](#) 

Top Industries

by visitors reading reviews

Financial Services Firm



Computer Software Company



Manufacturing Company

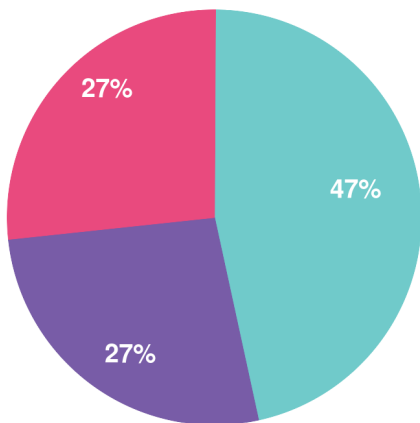


Healthcare Company

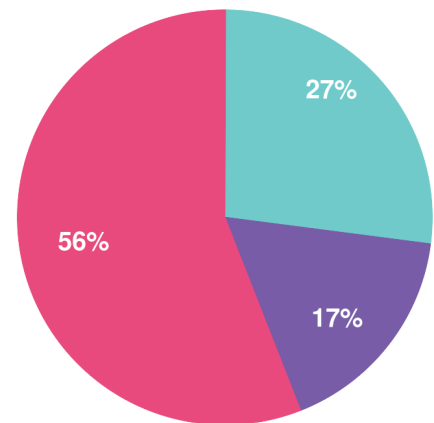


Company Size

by reviewers



by visitors reading reviews



Large Enterprise

Midsize Enterprise

Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944