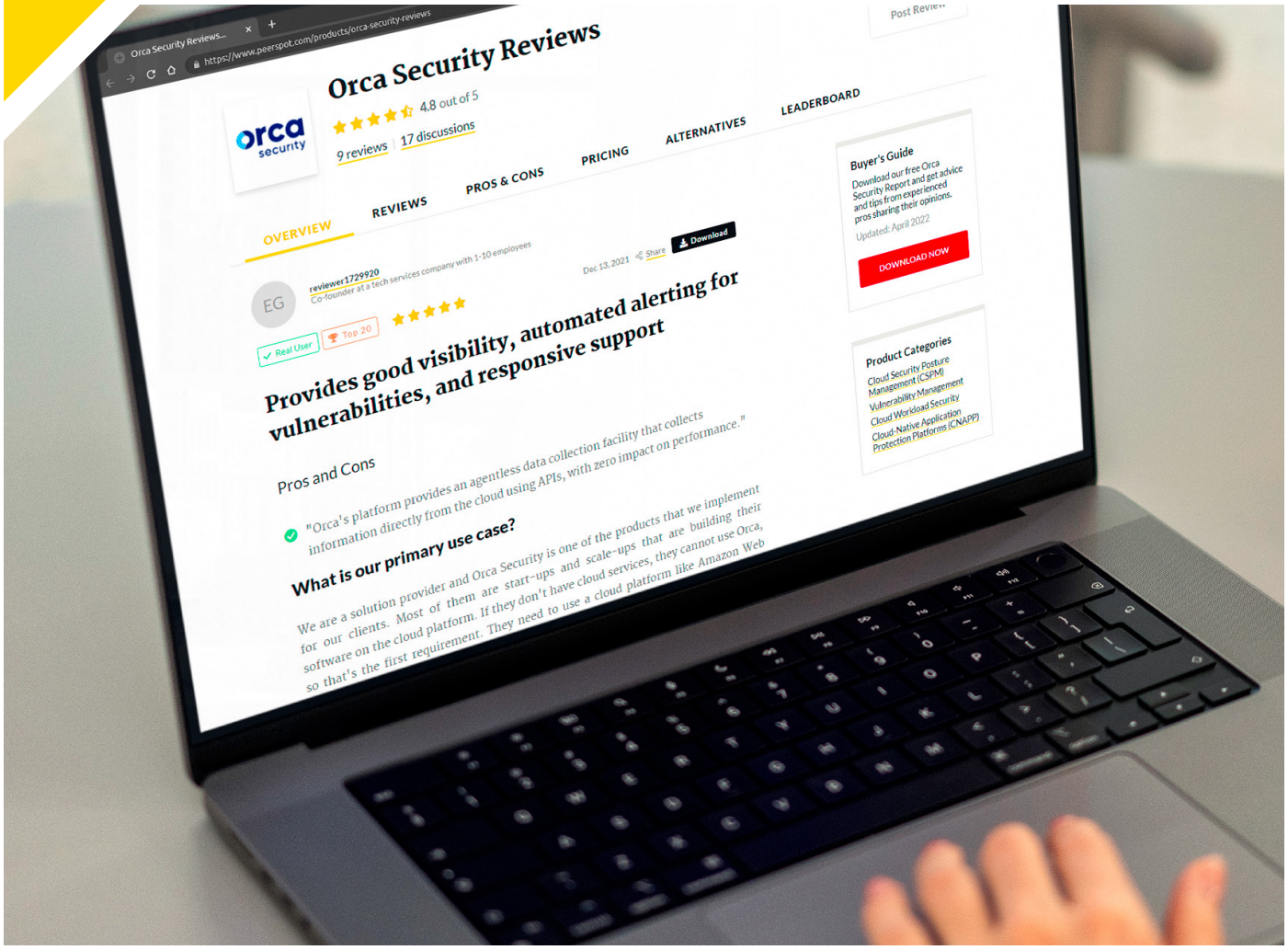
PeerPaper™ Report 2022

Based on Real User Reviews of Orca Security

How Orca Security Delivers on the CNAPP Promise



PeerSpot

Contents

Introduction

Orca Security has published a buyer's guide for organizations evaluating Cloud-Native Application Protection Platforms (CNAPPs). As cloud security evolves and the CNAPP category continues to emerge and gain interest among security teams, Orca published the guide to highlight the primary values of a CNAPP. The guide quotes a survey by 451 Research, which found 46% of respondents felt that security and compliance were their top concerns when using cloud-native technology. A CNAPP addresses the security risks associated with cloud adoption and use of cloud native application architectures, such as VMs, containers, Kubernetes and serverless computing.

Except where noted, the companies referenced in this paper have more than 500 employees.

The Buyer's Guide

The buyer's guide highlights five key considerations when selecting a CNAPP:

1. Consolidation of the capabilities of multiple tools in one platform
2. Agentless design
3. Context-aware risk prioritization
4. Continuous Integration/Continuous Deployment (CI/CD) security and integrations
5. Vendor support

The guide is intended to help IT departments, DevOps teams and security organizations address coverage gaps from traditional security tools. It provides insights that enable them to overcome difficulties in CNAPP deployment and get the value that CNAPPs should provide, including contextual risk prioritization, cloud visibility and alleviating "alert fatigue." The guide calls attention to issues that arise when security activities are not integrated with DevOps—a problem that can lead to the sub-optimal practice of performing security checks on applications after they are deployed to production.

Multiple tools in one

CNAPP Use Cases

PeerSpot members are putting Orca to work in a variety of use cases. For a CISO at a tech services company, "Orca is the inceptive tool that I deploy when I join a company." He said, "It will be one of the first things I do after an awareness training program." He does this because Orca serves the function of giving his team insights into the resting risk state as it combines so many signals without actually having to govern the assets. Orca tells them what they have and what needs to be updated. He added, "As soon as I have access to the AWS [Amazon Web Services] or GCP [Google Cloud Platform] or Azure accounts, I just drop Orca in and it shows me the abstract risk of everything in that cloud."

Securing workloads inside AWS is the use case for a Chief Risk Officer at a financial services firm. He said, "It secures all of our perimeter and AWS, as well as all of our databases, applications and transport. For every facet of AWS, right down to operating systems, we use Orca to take a look at it." A CISO at Lemonade Inc., an insurance company, uses Orca to identify threats and vulnerabilities, manage their cloud security posture and alert Orca's Cloud Security Posture Management (CSPM) to possible threat issues.

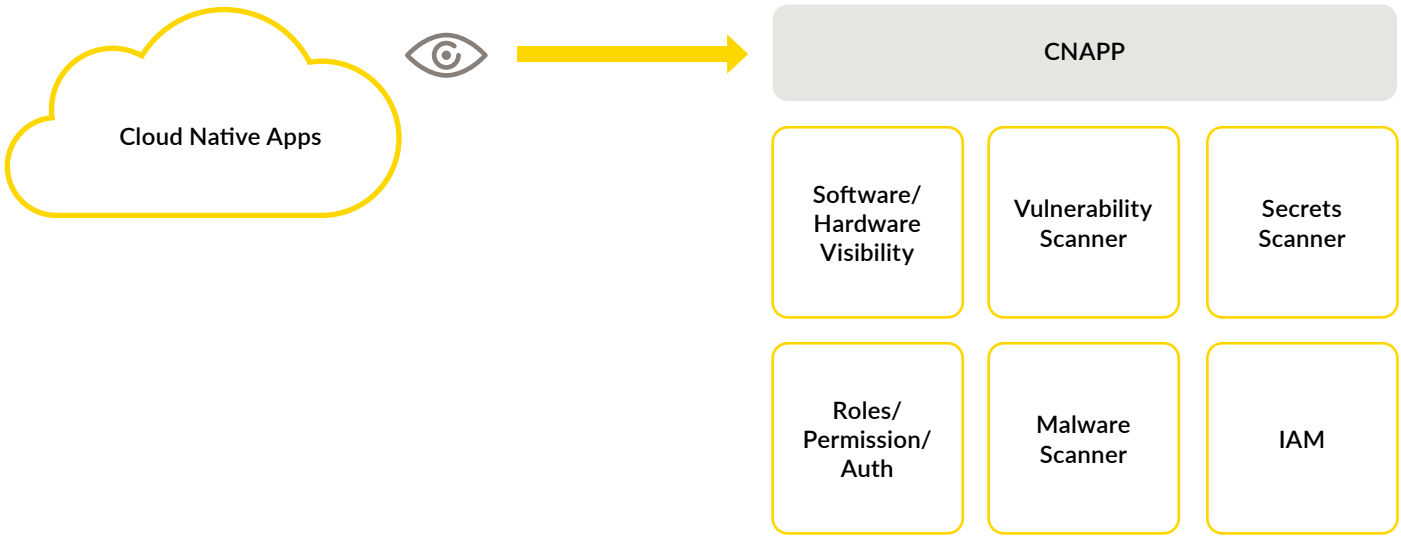
Consideration #1
Multiple Tools in One

As the buyer's guide sets out, the first consideration for selecting a CNAPP is to look for a solution that combines the work of multiple tools. The financial services Chief Risk Officer put it this way: "Orca provides X-ray vision into everything within the cloud properties, whereas normally, this would require multiple tools. As an analogy, for on-premises equipment, you would need different tools to be able to see the performance of a system, determine what versions of software applications are installed, and look at the security. You would need yet another one to give you a holistic view of all of the hardware inside of the system."

He then said, "From this one platform, we can get visibility right down into the hardware through all of the applications, and through the operating system. One application provides an entire view of our security." Figure 1 captures this idea.

> **"From this one platform, we can get visibility right down into the hardware through all of the applications, and through the operating system."**
>
> Read review »

Figure 1 - A CNAPP must combine the capabilities of multiple tools into one.



> "We had good timing when we picked Orca, rather than various tools to do the same job. If you have multiple scanners and you install Orca, you can remove the other ones."
>
> Read review »

"It solves the issue of having to run multiple tools, such as a vulnerability scanner, a secrets scanner, and a role management/permission/authorization tool that searches for abnormalities," said a CISO at a small recruiting/HR firm. He then went on to say, "I also like the fact that the solution includes the most potentially painful parts, out-of-the-box, like malware and secrets scans, IAM, attack vectors, and benchmarks against CIS and other best practices."

For this user, Orca helped them save money because his department did not have to acquire multiple tools to cover different aspects of cloud security. He said, "We had good timing when we picked Orca, rather than various tools to do the same job. If you have multiple scanners and you install Orca, you can remove the other ones. We didn't have anything, and Orca solved three or four different problems in a single tool."

Orca's agentless design enabled users to avoid multiple tools. A Chief Security & Trust Officer at SiSense, a software company, stated, "The agentless approach also means that we're able to avoid the need to deploy and maintain multiple tools." A Co-founder of a small tech services company similarly related, "By using the agentless approach, our clients avoid the need to deploy and maintain multiple tools."

Consideration #2
Agentless Design

The second consideration is to work with a CNAPP with an agentless design. Peerspot users were passionate about the value of this approach to cloud application management. According to SiSense's Chief Security & Trust Officer, Orca's agentless deployment led to very rapid time-to-value, without long and complex deployment requirements. As he said, "It took less than 24 hours, and we had intelligence and insight."

"Orca's platform provides agentless data directly from your cloud configuration with zero performance impact," explained the tech services CISO. He added, "It can analyze machines that I don't have access to. That in itself is the most game-changing thing I have seen, not just in security but in technology, in my 25-year career. Agents are a huge problem in security."

Agentless design

> "Orca provides the capability for agentless data collection directly from your cloud configuration and from the workloads' runtime block storage, which is one of the massive advantages of the tool."
>
> **Read review »**

Other notable comments about agentless design include:

- "Agentless approach makes it simple, reducing the number of tools we use, while rankings help focus our engineers. You don't have to implement anything. It takes five minutes to turn on. The biggest lesson I've learned from using Orca is that agents suck." - CISO at a tech services company with over 200 employees

- "Because of its agentless nature, there is zero deployment time. The deployment strategy is mostly, 'Choose the accounts that are there and then hookup Orca.' - Chief Security & Trust Officer at SiSense

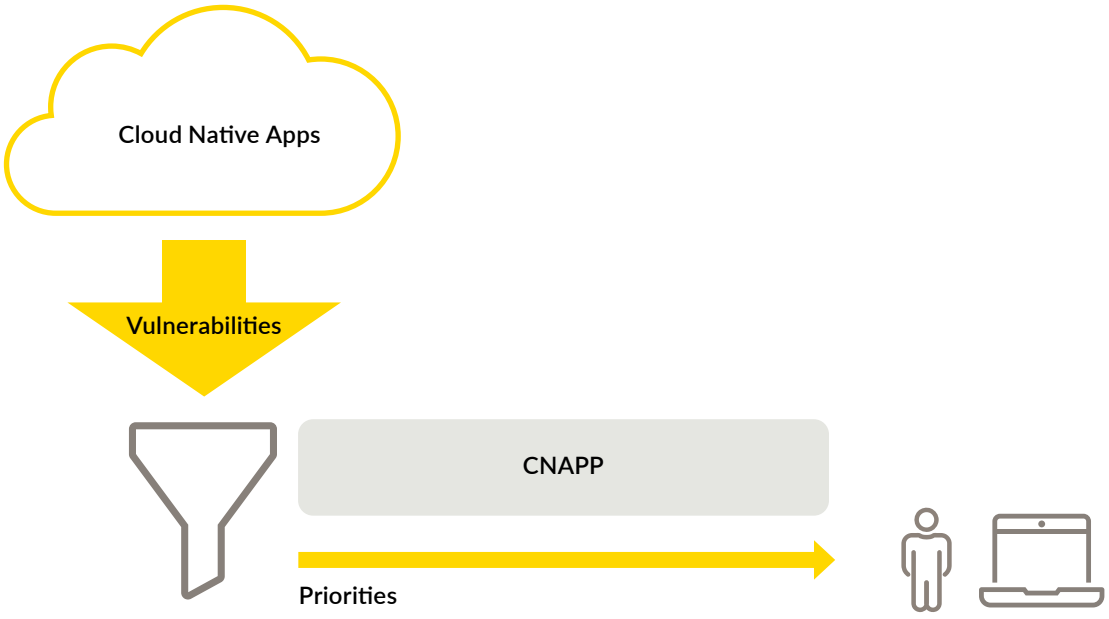
- "Orca provides the capability for agentless data collection directly from your cloud configuration and from the workloads' runtime block storage, which is one of the massive advantages of the tool. The tool gives us the ability to monitor things as we spin them up and as we tear them down. I can't state emphatically enough how important the agentless tool is." - Chief Risk Officer at a financial services firm

Consideration #3
Context-Aware Risk Prioritization

Securing cloud applications is more efficient and ultimately successful when security managers can establish a priority for dealing with risks. Not all risks are equal. Resources are limited. A CISO at a tech services company with over 200 employees described how his team had vulnerability system coverage but lacked a good ranking of priorities. The tools would scan the environment, but were unable to rank issues.

He said the system would tell the team, "We found 100 servers vulnerable to this CVE, so you should patch it." But, as he noted, "What they don't tell you is that there's no patch, or that your servers are down so you don't even have to. The information from those solutions was missing context and the ranking. You can get visibility with agents and there are a lot of ways to do that. But the ranking and the context across the entire environment, that is what is unique about Orca." Figure 2 depicts this kind of prioritization.

Figure 2 - Context-aware risk prioritization enables security analysts to focus on high priority issues.



> "The agentless and direct collection of data enables Orca to see assets within its environmental and business contexts and prioritize truly critical security issues."
>
> **Read review »**

"The agentless and direct collection of data enables Orca to see assets within its environmental and business contexts and prioritize truly critical security issues," said the financial services Chief Risk Officer. "This is one of the huge advantages of Orca. It sees everything in the environment and through its AI, properly categorizes what the threats are and shows them to you in a much better way. It aggregates all of the alerts and determines what's really important, and then shows them to you."

The benefit of this capability, in his view, was the reduction in the need for additional staff to investigate all of the alerts to try and determine what's real, what's critical, and what the actual problems are. "It does all of that work for you," he said.

Context aware risk prioritization can mediate the effects of alert fatigue. "The fact that it prioritizes vulnerabilities and findings, and doesn't present you with hundreds of unuseful findings, is important,"

said the CISO of the HR firm. "They focus the information and make you concentrate on the high-priority items. This is something that differentiates it from the others."

The tech services Co-founder echoed this idea, saying, "When you start reducing the vulnerabilities that you have, the number of alerts you are receiving will decrease compared to what it was in the beginning. It takes some time to achieve a healthy state of cloud security but once a baseline is achieved, you will immediately see the problem if there is a critical alert."

Consideration #4
CI/CD Security and Integrations

Cloud native applications need to be secure at the development stage. If they are not, there is the risk that vulnerabilities can make their way into production before anyone notices. For this reason, a CNAPP should integrate with CI/CD solutions used in software development and operations (DevOps). Lemonade's CISO shared an example of this capability, saying, "If we see an SSH key put up onto an externally facing machine by a developer, Orca will notify us, and we can deal with it immediately. Our other products don't tell us about that."

This user also acknowledged the value of Orca's agentless design in this context. The ease of deployment, "didn't require me to test it in different environments by DevOps." In his view, testing on DevOps environments would have added weeks to deployment.

Peerspot members also discussed how Orca enabled them to see security issues that were not visible to development teams. "It can even see into ODD [outcome driven development] and other activity logs that are not collected by default by DevOps," said the CISO of the HR firm. "It provides you with great visibility into each asset, including containers, storage devices such as RDS, CCS, and EC2, and S3. It gave us an edge over the DevOps team, because we saw way more compared to what they see."

"If we see an SSH key put up onto an externally facing machine by a developer, Orca will notify us, and we can deal with it immediately. Our other products don't tell us about that."

Read review »

This user then remarked, “It sees things very clearly and you get a notification, alerts to Slack or whatever system you are using. We have also exported the alerts to our Splunk environment, to cross-reference them with other systems as well. It provides great focus on the right and the most important topics that we should attend to first.”

Consideration #5
Vendor Support and Ratings

Excellent support

Quality of support also matters. Peerspot members affirmed that Orca backed up their product with good service. SiSense’s Chief Security & Trust Officer was pleased with the Slack channel devoted to Orca support. He said, “It’s real-time for us. If we have an issue, we go in and just message out, and then we can have that full loop within that Slack channel.”

The tech services CISO stated, "They give very good support to us. We don't need a lot of support, but sometimes we get audited and the auditors want a certain kind of format to the report. They are really helpful on that. If we're not sure about something or we have a question about containers, they're always very helpful. When there has been a new vulnerability and we wanted to make sure we're covered, they have been there for us every time."

"When you send an email, you get an answer immediately," revealed the tech services Co-founder. "They really try to determine what the problem is and identify the root cause. Either it's because it's something that we didn't know of, or were unable to find in the documentation, or it's a bug or feature that is not known yet." Lemonade's CISO likewise remarked, "Orca's support is extremely responsive and competent."

> **"They give very good support to us. We don't need a lot of support, but sometimes we get audited and the auditors want a certain kind of format to the report. They are really helpful on that."**
>
> **Read review »**

Conclusion

The CNAPP Buyer's Guide makes five recommendations for organizations looking at this type of cloud security solution. To address the security risks associated with cloud adoption and use of cloud native application architectures, a CNAPP should offer the functionality of multiple tools. An agentless design is critical, as it enables fast deployment and simple management. Context-aware risk prioritization cuts down on alert fatigue and helps security teams focus on issues that matter. CI/CD integration keeps vulnerabilities out of production code. And, strong vendor support is a "must have." With these factors in place, a CNAPP will make it possible to migrate and operate securely in the cloud.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Orca Security

Orca Security provides instant-on security and compliance for AWS, Azure, and Google Cloud—without the gaps in coverage, alert fatigue, and operational costs of agents or sidecars. Simplify cloud security operations with a single CNAPP platform for workload and data protection, cloud security posture management (CSPM), vulnerability management, and compliance.

Orca Security prioritizes risk based on the severity of the security issue, its accessibility, and business impact. This helps you focus on the critical alerts that matter most. Orca Security is trusted by global innovators, including Databricks, Autodesk, NCR, Gannett, and Robinhood. Connect your first account in minutes: https://orca.security or take the free cloud risk assessment.