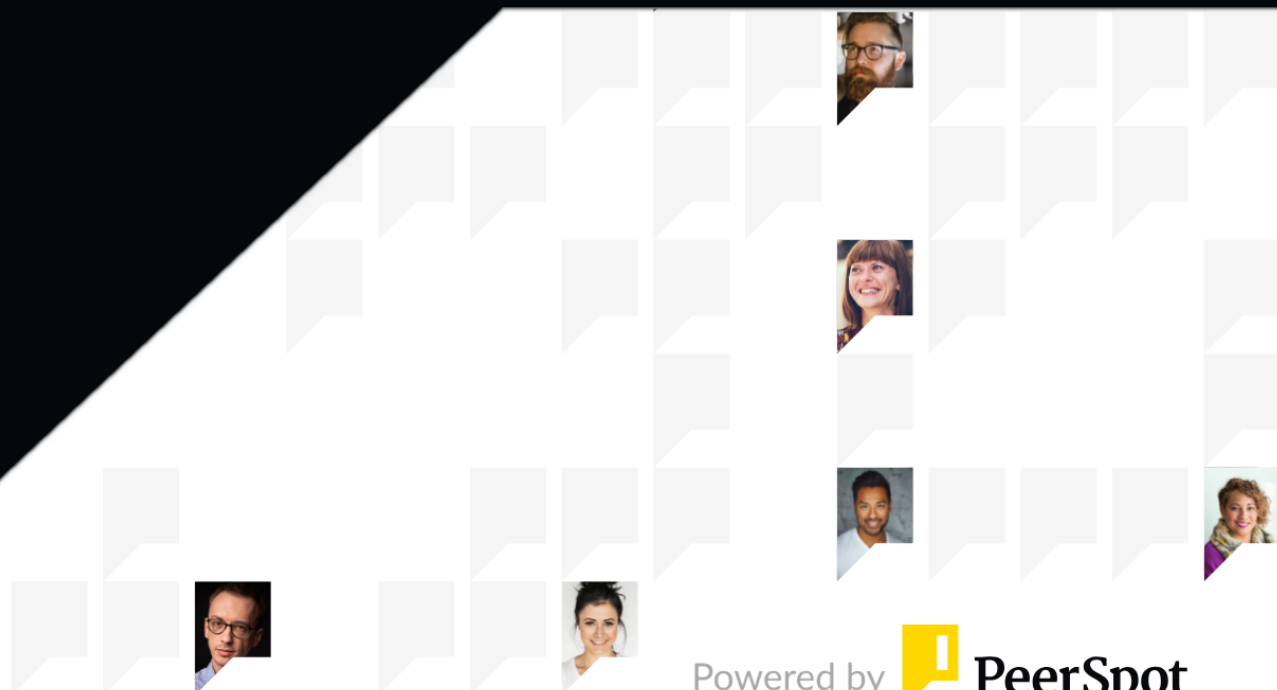




Aqua Cloud Security Platform

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16 - 18

Use Case..... 19 - 25

Setup..... 26 - 29

Customer Service and Support..... 30 - 31

Other Advice..... 32 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

Product Recap



Aqua Cloud Security Platform

Aqua Cloud Security Platform Recap

Aqua Cloud Security Platform supports container environments with strong features such as Docker and Kubernetes integration, efficient vulnerability management, and seamless runtime protection, making it a key choice for cloud and container security.

Aqua Cloud Security Platform focuses on comprehensive container and cloud security enhancements. It offers robust tools for Docker and Kubernetes, efficient vulnerability management, and on-demand patching. The platform is praised for its Runtime Protection, Drift Prevention, and robust documentation, promoting seamless integration with existing platforms. Image scanning, Digital Threat Analysis, and sandboxing services accentuate security measures while integration with Docker Hub ensures ease of use. Scalable runtime policies, image assurance, and dynamic threat analysis simplify security tasks. Challenges remain in developing web security portals and greater standard server integration. Enhancing reporting, simplifying training, and improving log forwarding are key goals. Resource consumption, clearer roles, automation, and code analysis are vital future considerations.

What are the most important features of Aqua Cloud Security Platform?

- **Docker and Kubernetes Support:** Ensures container security and streamlined operations.
- **Vulnerability Management:** Efficient scanning and on-demand patching.
- **Strong Runtime Protection:** Implements Drift Prevention and scalable policies.
- **Seamless Integration:** Works with existing platforms for optimal performance.
- **Image Assurance and Threat Analysis:** Provides thorough security checks and dynamic analysis.

What benefits or ROI can users expect?

- **Simplified Container Security:** Streamlines container and cloud tasks for enhanced protection.
- **Enhanced Image Assessment:** Detects configurations and risks efficiently.
- **Greater Data Protection:** Ensures application visibility and security in deployments.
- **Flexible Licensing Models:** Offers potential for reconsideration and optimization.

Aqua Cloud Security Platform is leveraged in industries focusing on container security, vulnerability scanning, and securing Kubernetes configurations within CI/CD pipelines. It is employed for image assessments and network security, demonstrating its efficacy in cloud applications and workload protection. Efficiently identifying misconfigurations and risks in cloud environments, it provides scanning for public clouds and docker environments, emphasizing data protection and application visibility tailored to customer-specific deployments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “From the ROI perspective, Aqua Cloud Security Platform provides value from day one in terms of identifying the posture of the environment, identifying vulnerabilities, and faster remediation.”



Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

- ✓ “From my point of view, it is a pretty good thing because it is not something that works all the time as a microservice addition, it does not increase costs or resources, and that is good.”



Dmytro Volobuev

DevOps Engineer

- ✓ “Aqua Cloud Security Platform is perfect for us because it has container image scanning, real-time protection, Kubernetes security, and inbuilt cloud security, making it an all-in-one tool.”



DeepakReddy

Sr.Devops engineer at Scaler

- ✓ “Among the features I have shared, the ones I find most valuable are the CI/CD integration since it allows security checks to happen early in the development cycle.”



Henry Mwawai

Information Security Engineer at a consultancy with 11-50 employees

- ✓ “Since adopting Aqua Cloud Security Platform, I have observed around a 40 to 45 percent increase in productivity and a reduction of around 35 to 40 percent in time taken for tasks that previously required manual intervention, such as Python linting.”



Sayed Basha

IT platform engineer at Infosys via consign Space Solutions pvt ltd

- ✓ “Aqua Cloud Security Platform positively impacted my organization by allowing deployment from code to cloud in the entire CI/CD pipeline, with excellent capabilities and recent AI application security that is useful in the DevSecOps platform.”



Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees



“Aqua Cloud Security Platform has positively impacted my organization by helping with decreasing the number of compliancy issues with the company that we were working on.”



Mark Rausch

Cloud Security Support at a tech vendor with 501-1,000 employees

What users had to say about valuable features:

What I like the most about Aqua Cloud Security Platform is that as I understand it, it is a pretty lightweight service and the sidecar container cannot fail because it is actually doing nothing other than bringing a binary. From my point of view, it is not a bottleneck and it is not a wrapper that can fail. As I understand it, it just scans the container on start and then does nothing. There is no extra load and no extra resources. I think it is pretty light. From my point of view as DevOps, it is a pretty good thing. It is not something that works all the time as a microservice addition, it does not increase costs or resources, and that is good.

Dmytro Volobuev

DevOps Engineer

[Read full review](#)

“The best features I can identify are container image scanning, Kubernetes security, runtime protection, CSPM, infrastructure as code security, and supply chain security as well.

“Not specifically cost saving, but from the security side, we completed our compliance standards, and in our CI/CD pipeline, we set up our security gates between the planning, build, and code phases..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

The best features Aqua Cloud Security Platform offers are the depth at which container and Kubernetes security is covered, including image assurance and scanning, along with very strong runtime protection with drift detection and prevention.

Regarding how runtime protection and drift detection have helped my team, as any drift detection mechanism does, it helps identify if anything has been changed in production that is not reflected in code, and when that happens, an alarm is triggered.

“Aqua Cloud Security Platform has positively impacted my organization by significantly increasing productivity and helping identify the security posture of my environments, which releases a lot of pressure from the security team.

“My productivity increased mainly because time to production has been reduced, thanks to the drift detection and malware analysis at runtime, allowing my team to react faster before reaching production. .”

Francisco Pulido

SecOps Engineer at a real estate/law firm with 501-1,000 employees

[Read full review](#) 

“The best features found in Aqua Cloud Security Platform include capabilities at the domain-wise level, which include CWPP, secret detection, runtime protection, Kubernetes security, vulnerability management, and CSPM.

“Aqua Cloud Security Platform positively impacted my organization by allowing deployment from code to cloud in the entire CI/CD pipeline, with excellent capabilities and recent AI application security that is useful in the DevSecOps platform.

“Multi-cloud support with AWS, Azure, GCP, and software supply chain security with SBOM generation and CI/CD pipeline scanning are unique aspects that set Aqua Cloud Security Platform apart..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“The best features that Aqua Cloud Security Platform offers are Kubernetes security, cloud-native vulnerability management, risk prioritization, and real-time protection. Other features include CI/CD integration and compliance reporting, which helps security as a whole.

“Among the features I have shared, the ones I find most valuable are the CI/CD integration since it allows security checks to happen early in the development cycle. This enables me to identify vulnerable dependencies, insecure container configurations, and other issues before they reach production, helping me reduce the risk before deployment occurs as I am able to identify security weaknesses before deployment happens.

“I have a software engineering team, and before providing a client with a fully deployed application, Aqua Cloud Security Platform helps us know any vulnerabilities and patch them. It highlights any misconfigurations in place before deployment. It also helps in risk prioritization, where the security team focuses on vulnerabilities based on context rather than treating every finding equally. Aqua Cloud Security Platform integration helps security issues in the pipeline be detected earlier, enabling us to perform runtime monitoring and check for any indicators of compromise earlier..”

Henry Mwawai

Information Security Engineer at a consultancy with 11-50 employees

[Read full review](#) 

“Aqua Cloud Security Platform is perfect for us because it has container image scanning, real-time protection, Kubernetes security, and inbuilt cloud security. It is an all-in-one tool.

“The best feature of Aqua Cloud Security Platform is the Kubernetes security, which secures admission controllers, runtime policies, namespace protection, and RBAC and pod security. It helps manage all these aspects effectively with this cloud-native security tool.

“We use admission controllers, and this Aqua cloud-native solution has inbuilt admission controllers and Kubernetes operators that help secure our Kubernetes pods, deployments, and services. This is particularly beneficial for us, especially because other solutions operating in the same space do not match the accuracy and operational capability. The scans and benchmarking are also very good.

“Other notable features I found in Aqua Cloud Security Platform include multiple integrations with tools such as Docker, AWS, Azure, Google Cloud, GitHub, GitLab, Jenkins, Azure DevOps, Bitbucket, Terraform, and Jfrog. There are hundreds of integrations available. It also has multiple deployment options such as hybrid cloud, multi-cloud, or on-premise, and includes SAST with all security tooling inbuilt, making it a comprehensive tool.

“The dashboard shows all the important information we were missing in our previous tool..”

DeepakReddy

Sr.Devops engineer at Scaler

[Read full review](#) 

Other Solutions Considered

“We looked into other options. There's lots of competition out there. There is NGINX, for example, or we can do container security via AWS or GCP. However, we have a hybrid environment, and Aqua accommodates us in that sense. .”

Dharmendra Kr. Chauhan

[Read full review](#) 

Manager|Cloud Security & Solution Architect| CloudOps|AppSec |
DevSecOps | DevOps | CapOps | FinOps at Wipro

“Aqua Security is an on-demand service. Swisslog just launched a product, but it is not as good as Aqua Security in terms of accuracy. Swisslog is integrated with the package and with Aqua Security, you need to pay more for the first scan..”

OshinSharma

[Read full review](#) 

Head - Cybersecurity at a retailer with 1,001-5,000 employees

I have never used any alternatives to Aqua Cloud Security Platform that I can compare it with. I did not use it before. However, I was thinking about how it would work with a container that is already wrapped with some monitoring system or system that also scans containers. I did not meet one, but there is sometimes a pretty popular thing that also scans containers for counting system and load monitoring.

Dmytro Volobuev

[Read full review](#) 

DevOps Engineer

“We evaluated various options, including Snyk and Splunk, as well as other tools such as Trivy. We found Aqua Cloud Security Platform to be the best choice among all alternatives..”

DeepakReddy

Sr.Devops engineer at Scaler

[Read full review](#) 

“We previously used a security tool built into our company, which had many issues, mainly only supporting AWS and Docker, without Kubernetes or other cloud providers. That is why we switched to Aqua Cloud Security Platform, an all-in-one solution..”

DeepakReddy

Sr.Devops engineer at Scaler

[Read full review](#) 

“Previously, we were using multiple tools for scanning: container image scanning, Kubernetes security, runtime security, CSPM and on the IAC side. We were using multiple scanning tools for that. Then we found one single solution, which is Aqua Cloud Security Platform. So it really added value for our organization.

“We were previously using a lot of open-source tools. Open-source tools have their limitations and there is no vendor support. Then we did a lot of analysis with multiple paid solutions and came to know that Aqua Cloud Security Platform is the best from our environment's perspective..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“There was definitely some time saved with Aqua Cloud Security Platform. The ability to quickly go through and find out what needed to be done allowed us to quickly put reports together to present to the client..”

Mark Rausch

[Read full review](#) 

Cloud Security Support at a tech vendor with 501-1,000 employees

“As I said, manually checking vulnerability is not really feasible. We had to have some kind of solution. The ROI is clear. We could not live without it. Now we are getting back a picture of the vulnerability and we are able to fix severe security/vulnerability bugs..”

Verified user

[Read full review](#) 

Director of Engineering at a tech vendor with 51-200 employees

“I have seen a return on investment with Aqua Cloud Security Platform as it provides good capabilities. It is generally used for the DevSecOps pipeline to scan the entire SAST, DAST, or ISC, performing excellently in that area..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“I'm not sure if I can place any numeric values on ROI but, considering that we went from zero security to having full visibility and the ability to create policies to enforce our requirements, I think it was a reasonable investment. Going from zero to, say, 80 to 90 percent capabilities was a good deal..”

Cem Gurkok

Lead Security Engineer at a tech company with 10,001+ employees

[Read full review](#) 

“I have seen a return on investment mainly through time savings and early identification of security issues rather than reducing headcount. Aqua Cloud Security Platform helped automate vulnerability and misconfiguration scanning. I would prefer to quantify the financial savings using an organization's actual deployment and remediation data rather than provide an estimation figure. The main measurable benefits are faster identification and remediation of findings, fewer issues progressing to later stages, and reduced manual effort for repetitive security checks..”

Henry Mwawai

Information Security Engineer at a consultancy with 11-50 employees

[Read full review](#) 

“From the metrics perspective for Aqua Cloud Security Platform, I can say that faster deployment and faster vulnerability remediation reduced time to fix vulnerabilities early in the pipeline. The impact can reduce remediation effort by 40% to 60%, avoiding production-level fixes which are costlier. Breach risk detection through runtime protection plus compliance reduces the risk of attack by 30% to 40%. Tool consolidation is another aspect where replacing multiple tools such as scanners, runtime compliance tools, and others can reduce tool cost by 15% to 25%.

“From the ROI perspective, Aqua Cloud Security Platform provides value from day one in terms of identifying the posture of the environment, identifying vulnerabilities, and faster remediation. Remediation effort improved by at least 40% to 60%. Breach risk reduction is significantly increased by 30% to 50%. Regarding tool consolidation, I do not need different tools, especially for the DevSecOps pipeline perspective, as one tool can suffice for scanning, runtime, and compliance functions. When consolidating tools, costs reduce around 15% to 25%..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[Read full review](#) 

Use Case

My main use case for Aqua Cloud Security Platform is container and Kubernetes security across the full life cycle, including image scanning for vulnerabilities, malware, and secrets in CI.

For example, I use Aqua Cloud Security Platform for scanning container images through my registries, specifically Docker Hub, and I scan them before deployment. I have policies that are set to fail a build or a PR when any critical or high CVEs appear. .”

Francisco Pulido

SecOps Engineer at a real estate/law firm with 501-1,000 employees

[Read full review](#) 

“Aqua Cloud Security Platform secures our containers, Kubernetes clusters, and container images. We regularly run container image scanning, SAST scans, and vulnerability management and software supply chain security scans. We also use it for secret detection, rotation of secret keys, and compliance monitoring.

“Aqua helps with secret detection by scanning our GitHub or GitLab repositories to check whether there are any passwords or sensitive data present. If it detects them, we remove them or take action around them..”

DeepakReddy

Sr.Devops engineer at Scaler

[Read full review](#) 

“My main use case for Aqua Cloud Security Platform was looking at the code-based pipeline to find vulnerabilities in place. I was using it for DevSecOps, where I checked for misconfiguration around pipelines and across my cloud environments.

“One specific example from when I was using Aqua Cloud Security Platform to find vulnerabilities was scanning container images as part of my pipeline. For the Docker build for a Python application, it was scanned before deployment and Aqua identified vulnerable packages and misconfiguration issues in the image. I reviewed the findings, prioritized the critical and high vulnerabilities, then updated the affected dependencies and Docker configuration, and performed a rescan to confirm the issues had been resolved before deployment..”

Henry Mwawai

Information Security Engineer at a consultancy with 11-50 employees

[Read full review](#) 

“Aqua Cloud Security Platform is primarily used for cloud-native applications, focusing on cloud identity and entitlement management and vulnerability management for containers, Kubernetes, and ISC, along with secret detection and DevSecOps.

“A recent project with Aqua Cloud Security Platform addressed a security challenge related to container and Kubernetes security using runtime protection. Examples include container escape attempts, privilege escalations, reverse shell executions, malicious process wrapping, and crypto mining, which involved using Aqua runtime controls to scan the entire CNAPP.

“Kubernetes security is a key focus, where Aqua provides capabilities for network segmentation, pod security controls, and service account monitoring, often stronger than Microsoft Defender for Cloud and more mature than Orca..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“I used Aqua Cloud Security Platform for container image scanning, runtime threat detection, infrastructure as code scanning, and software supply chain security.

“I used it for container image scanning registries for our Azure cloud environment and AWS ECR as well. So it was for Azure Container Registry scanning and Amazon ECR scanning.

“For Kubernetes security, I think it is a good feature, including RBAC analysis, privileged containers, host path detection, and pod security. And on the CSPM side as well.

“Mostly, I used it for container scanning and our CI/CD pipeline scanning. So mostly, on the CSPM side.

“We deployed it in a hybrid environment. We also have both AWS cloud and Azure cloud. So it is a hybrid deployment..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

I wrote a setup process for Aqua Cloud Security Platform during a short-term contract with the company, and I probably used it for around one month after installation.

Aqua Cloud Security Platform was a piece of microservices on AWS Elastic Container Service with a few microservices, something around maybe 100 or 150 containers representing different parts of services of the company. It was really different because it was a few different services. I was writing implementation as a DevOps engineer and developer of infrastructure rather than as a user.

“It was easy only on the test stage with Aqua Cloud Security Platform where I could run manual tests and verify it was working. However, we were too optimistic about how much time the implementation should take. I had to rewrite a lot of Terraform modules because every container needed to be updated. The most difficult things compared to our expectation were that the last simple step of updating the entry point proved extremely complex. Every module, every build, and every container was reviewed and rewritten. I had to rewrite builds and deployments because it was a pretty big system that was highly automated and had been done by different people at different times with different scripts in Bash, Python, and Terraform. Some things were updated manually in Terraform, so the entry point was probably the most tricky part because it involved Java microservices with some entry points that were scripts and some entry points that were huge terrible lines with everything related to Java starts that sometimes looked a poem. I had to move all this content to the command line, which was tricky as a syntax and as a part of the build process. Some entry points were already patched in the entry point at container startup in the module, which made it pretty tricky.

“It was not only ECS; my part was ECS while someone was working in EKS and we had discussions and testing on how to move it better with a lot of experiments because different entry points were patched, updated, scripted, or endless lines. It took pretty much time, and it was also complicated by company processes because different departments had different procedures for implementation. It took, with all these experiments, probably about four months to push it through all processes because some departments had up to four environments with procedures, QAs, testing, and all this. It was definitely more than one month that I estimated at the very beginning, but that was mostly due to company processes. If I had worked

there a couple of years before, I would not have estimated one month, and if I had full knowledge of processes and experience with implementation, I would have approached it differently.

“It was more tricky because I was new to the company and had to learn not only Aqua Cloud Security Platform but much more. I had to learn all modules, procedures, and processes, which was good. I jumped into infrastructure in a way that was a pretty good learning experience because I learned everything: build, deploy, infrastructure, and procedures. I pushed all this up to production and started in production, which is a pretty good line in my resume. .”

Dmytro Volobuev

DevOps Engineer

[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.

“Regarding the initial setup of Aqua Cloud Security Platform, the first area needing improvement is the complex initial setup. Deployment and configuration can be complex, especially in large environments that require skilled resources. For Kubernetes environments, initial onboarding and policy setup takes time. Compared to Wiz onboarding, it is not very straightforward, as I have also worked with Wiz..”

Samir Paul

Security Practitioner at a tech vendor with 10,001+ employees

[Read full review](#) 

“The initial setup was straightforward. The first time you deploy you, you need support but after that, it's easy to understand the documentation that they provide. After two or three times it's easy.

It takes around one week to get all of the environments in place but to do a PoC is only two days. .”

Verified user

Security manager at a tech services company with 11-50 employees

[Read full review](#) 

“The main trend is for deployment complexity, so we still have to use multiple resources for that. But after deploying it in the CI/CD pipeline, it enhances our CI/CD or automation capability for the organization. So the DevSecOps capacity or DevSecOps integration is good. And the supply chain security is also fantastic. Container security, Kubernetes security, runtime protection, everything is fantastic..”

Sudheer Kumar

[Read full review](#) 

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

“The initial setup is a little bit complex for an on-premises deployment. We needed to have many specialized people on Kubernetes to maintain this deployment and keep it up to date. It is a little bit complex because of Kubernetes, not because of Aqua itself, but Aqua have some features to facilitate the deployment.

You need three or four people for the deployment. For a small environment, deployment would take two to three hours. For larger environments, it would take longer than that.

This is an easy solution to maintain. The main thing is to maintain the databases..”

Verified user

[Read full review](#) 

Sales Engineer at a computer software company with 51-200 employees

“The initial setup was pretty straightforward.

If it is deployed from scratch, the documentation is pretty straightforward. We just followed the steps and we were able to do it. There were no unexpected bugs or any other issues we faced. Everything was quite straightforward.

I'd rate the solution four out of five in terms of the initial setup.

Maintenance was taken care. Maintenance was good there. It doesn't need any more effort. What we used was the latest one, a stable version, and since we were dealing with a corporate organization, we wanted stable versions to be always tested. .”

MohammedAsad

DevSecOps Engineer at Foodhub

[Read full review](#) 

“Initially, we had some issues. There were problems with Microsoft and AI. In the latest Aqua release, we did a multi-cloud deployment, and we coordinated the cloud and the migration.

There are a couple of components to contend with. For example, there's the Aqua gateway. It's fine to work with. However, it's hard to have control.

It's not overly complex. It just really depends on the environment. Therefore, it could be easy, or a little more complicated.

Mostly, my experience was pretty good. I'd rate it a 4.5 out of five in terms of ease of setup..”

Dharmendra Kr. Chauhan

[Read full review](#) 

Manager|Cloud Security & Solution Architect| CloudOps|AppSec |
DevSecOps | DevOps | CapOps | FinOps at Wipro

Customer Service and Support

For support related to Aqua Cloud Security Platform, I would rate it a 10 because I did not have a support request that was not handled. If I got an answer in a couple of days, it was probably even faster.

Dmytro Volobuev

DevOps Engineer

[Read full review](#) 

“Customer support is acceptable. Sometimes we receive a complaint from our L3 or L2 engineers that they are not getting proper on-time support, but overall, it is acceptable..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“The customer support for Aqua Cloud Security Platform is excellent, available 24/7, and provides better solutions for any issues raised through tickets..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“The technical support is highly responsive and exceptionally helpful. When I report an issue, they address it promptly and efficiently. I would rate it ten out of ten..”

Burak AKCAGUN

Business Development Manager at Axoft Ukraine

[Read full review](#) 

“In general, the support for this solution is good. It could be improved if it catered for customers in different countries to meet their specific demands. .”

Verified user

Sales Engineer at a computer software company with 51-200 employees

[Read full review](#) 

“I believe I only had one or two tickets open with customer support while I was working on Aqua Cloud Security Platform and everything seemed fine and quick.

“On a scale of one to ten, I would rate the customer support for Aqua Cloud Security Platform a ten out of ten..”

Mark Rausch

Cloud Security Support at a tech vendor with 501-1,000 employees

[Read full review](#) 

Other Advice

“My advice would be that if someone is looking for runtime protection, Kubernetes security, container security, IAC security, and supply chain security for their organization, then I think Aqua Cloud Security Platform is fantastic. But if they are looking for agentless assessment, attack path analysis, and ease of deployment, then they can look at other vendors. I would rate this product seven out of ten..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

Overall, I would give Aqua Cloud Security Platform a score of 7 to 8 because I do not know how it will behave in all situations. For example, a network problem with connectivity to an image or if Aqua Cloud Security Platform binary will not be able to connect to somewhere could be an issue. Some environments are highly hidden under VPCs, so some security changes can cut off a route to Aqua Cloud Security Platform repository or something similar. Someday it can be a surprise. I cannot predict how Aqua Cloud Security Platform is going to work and how long it can handle this. Regardless, there will be a delay and it can break any kind of post-start checks or something else. There are a lot of things I can imagine breaking. My overall rating for this review is 8 out of 10.

Dmytro Volobuev

DevOps Engineer

[Read full review](#) 

“The AI output of Aqua Cloud Security Platform is good, but I believe it can be improved. We received alerts about vulnerabilities in our dashboard, particularly related to a database call issue. The AI identified a problem with a Postgres snapshot, which turned out to be accurate, but it could be enhanced by including specific details about what has gone wrong.

“Aqua Cloud Security Platform needs some improvement in the UI, which is somewhat overwhelming, and the licensing can be expensive at scale. I gave this product a rating of eight..”

DeepakReddy

Sr.Devops engineer at Scaler

[Read full review](#) 

Regarding Aqua Cloud Security Platform's AI capabilities, I think its governance is lifecycle oriented, and although it has been implemented relatively recently, I have not had a huge opportunity to test it yet.

Concerning the accuracy and reliability of its AI capabilities, I can say that the scanning accuracy of the AI in Aqua Cloud Security Platform is quite good for catching CVEs that other tools have otherwise missed.

“My advice for others looking into using Aqua Cloud Security Platform is that it requires a big and mature security team or at least someone with enough experience in Aqua security in order to get the most out of it. I gave this product a rating of eight. .”

Francisco Pulido

SecOps Engineer at a real estate/law firm with 501-1,000 employees

[Read full review](#) 

“My advice for others looking into using Aqua Cloud Security Platform is that for

container security, Kubernetes security, runtime protection, supply chain, or overall [CNAPP](#), if someone wants to use it at a lesser price, this product provides good capabilities. They can proceed with this product; however, for dashboard and executive reporting, if that is specifically what you are looking for, you may want to consider other products.

“Aqua Cloud Security Platform's AI capabilities provide good governance and security primarily through risk prioritization, although compared to Wiz, Prisma Cloud, and Orca, it is less competitive at the moment. In terms of supply chain securities, Aqua Cloud Security Platform is paramount in comparison to other vendors.

“When it comes to the accuracy and reliability of Aqua Cloud Security Platform's AI capabilities, more work on the AI security side is required. A responsible AI part is missing, making it less valuable.

“I rated this product a seven out of ten..”

Sudheer Kumar

Cyber Security Practice Lead at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“The advice I would give is to base it on someone's specific cloud and [DevSecOps](#) requirements, then start with the areas with the most risk, such as container vulnerabilities, Kubernetes security, or CI/CD pipelines. I recommend piloting before wider deployment, as someone should assess the quality of its integration, reporting, remediation workflows, and how well it fits with their existing security processes.

“I think AI governance and security are important to evaluate regarding Aqua Cloud Security Platform. While there are controls for data privacy, access permissions, and transparency, Aqua Cloud Security Platform could strengthen its AI governance and security by providing more visibility into how AI recommendations are generated, what data is processed, and adding controls for

validating AI-driven security decisions before automated actions are taken, including transparency of AI-generated findings and ensuring human oversight.

“I find the output from Aqua Cloud Security Platform generally useful for speeding up security analysis and it helps prioritize findings. I would still validate the AI-generated recommendations against the underlying scan results and security context before taking action. For me, its value is high as an analyst assistant tool rather than something that should replace human validation. I would rate this review an eight out of ten..”

Henry Mwawai

Information Security Engineer at a consultancy with 11-50 employees

[Read full review](#) 

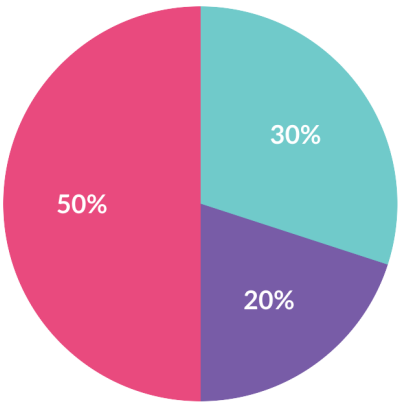
Top Industries

by visitors reading reviews

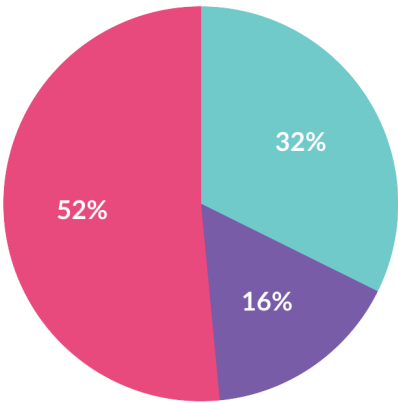


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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