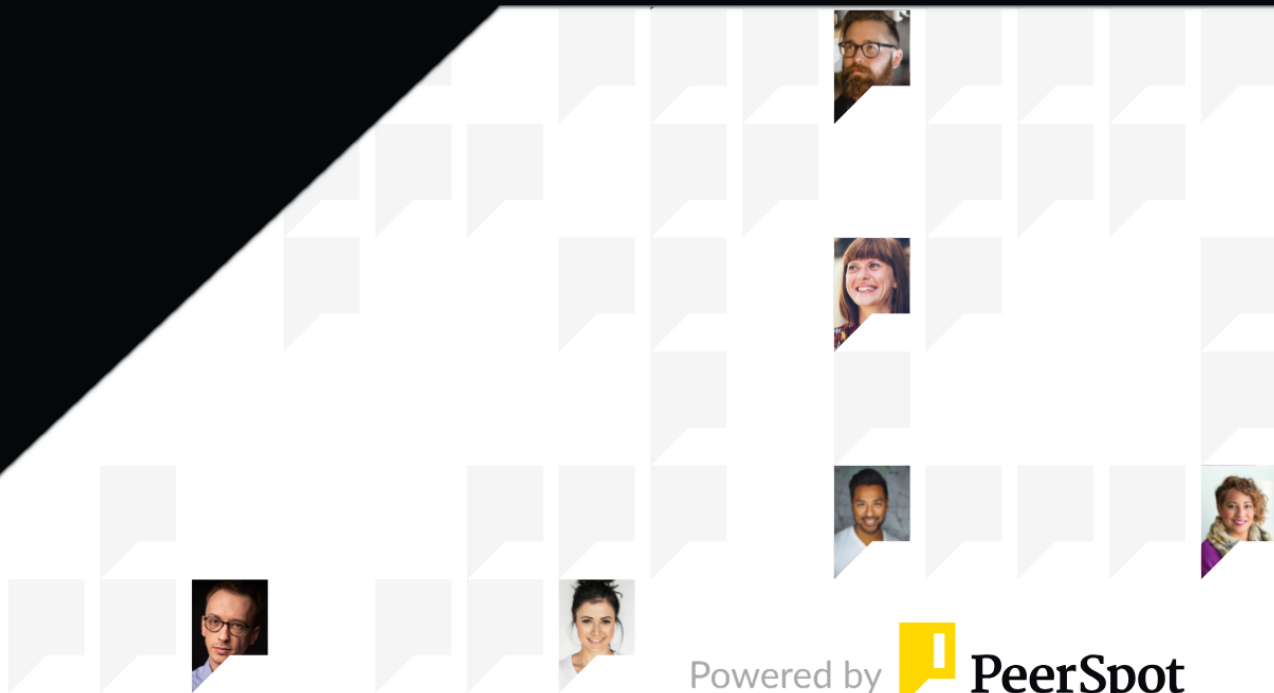




Qualys TotalCloud

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 14

Other Solutions Considered..... 15 - 17

ROI..... 18 - 20

Use Case..... 21 - 26

Setup..... 27 - 29

Customer Service and Support..... 30 - 32

Other Advice..... 33 - 37

Trends..... 38 - 39

About PeerSpot..... 40 - 41

Product Recap



Qualys TotalCloud

Qualys TotalCloud Recap

Qualys TotalCloud enhances security posture across cloud environments with continuous monitoring, vulnerability management, and risk visualization, ensuring efficient threat assessment and automated remediation for improved cyber risk reduction.

Qualys TotalCloud offers a robust suite of security tools essential for organizations managing multi-cloud infrastructures. By integrating cloud accounts and automating workflows, it supports AWS, Azure, and GCP, offering comprehensive vulnerability management and zero-day detection. The platform's user-friendly design, combined with its extensive risk management and unified threat assessment capabilities, enables organizations to prioritize and remediate vulnerabilities effectively. TruRisk Insights provides clear insights on cyber risks, while the automation options streamline patch management and scanning processes. API integration across IaaS and SaaS environments further enhances resource allocation efficiency and saves time, addressing misconfigurations across cloud environments.

What are the most important features of Qualys TotalCloud?

- **Accurate Vulnerability Reports:** Delivers precise and actionable insights for risk mitigation.
- **Zero-Day Detection:** Identifies and addresses zero-day vulnerabilities proactively.
- **Unified Threat Assessment:** Offers comprehensive evaluation of threats across the environment.
- **Extensive Risk Management:** Manages risks effectively with advanced insights and prioritization.
- **Continuous Monitoring:** Provides non-stop surveillance for vulnerabilities and threats.
- **Cloud-Native Automation:** Streamlines processes and reduces manual efforts using automation.
- **FlexScan for Internet-Facing VMs:** Scans external VMs efficiently to detect vulnerabilities.
- **Dashboard Risk Visualization:** Clear visualization helps prioritize vulnerabilities.

What benefits and ROI should users look for?

- **Improved Security Posture:** Enhances threat detection and response across clouds.
- **Time Savings:** Automation reduces time spent on manual vulnerability management.
- **Resource Efficiency:** Better allocation of resources through streamlined workflows.
- **Enhanced Risk Prioritization:** Focus on critical vulnerabilities for effective mitigation.
- **Integrated Cloud Accounts:** Facilitates seamless cloud management and security.

Qualys TotalCloud is deployed in sectors needing rigorous vulnerability management, such as finance and healthcare. Companies utilize it to secure multi-cloud environments like AWS, Azure, and GCP, focus on compliance, and integrate security into CI/CD pipelines to detect

and remedy threats pre-deployment.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Once it is set up, Qualys has proved to be one of our greatest assets.”



Verified user

Sr Security Engineer at a tech vendor with 5,001-10,000 employees



“Qualys TotalCloud has positively impacted our bank's performance, and we have definitely seen benefits after implementing this solution.”



Robert Orłowski

IT Security Expert at Alior Bank S.A.



“Qualys TotalCloud is overall the best tool available in the market for scanning purposes.”



Sanchit Makkar

Dns architect at a outsourcing company with 5,001-10,000 employees

- ✓ “Qualys TotalCloud has saved our time by giving us better asset visibility and risk-based prioritization, as it has reduced the time spent manually reviewing CVEs and deciding what to address first.”



Verified user

Soc Analyst at a manufacturing company with 10,001+ employees

- ✓ “In my opinion, this is the best tool.”



Verified user

Systems Engineer at a financial services firm with 10,001+ employees

- ✓ “The biggest strengths of Qualys TotalCloud are that it is pretty good at cloud visibility, has easy integration, and also has multi-cloud compatibility.”



Verified user

Senior security analyst at a manufacturing company with 10,001+ employees

- ✓ “Qualys TotalCloud helps you not just to identify misconfigurations, but you can actually also fix issues.”



MiracleChukwudebe

Cybersecurity Leader / Consultant at Ethnos IT Solutions

What users had to say about valuable features:

“Qualys TotalCloud helps you not just to identify misconfigurations, but you can actually also fix issues. You can see issues, identify misconfigurations within your cloud infrastructure, and be able to timely fix these issues.

Some other features I enjoy with Qualys TotalCloud include its integration with Qualys TruRisk, which allows you not just to identify vulnerabilities but to match them to specific use cases, specific signatures, and tell you what to prioritize when fixing them. Qualys TruRisk helps you prioritize issues. It does not just read one vulnerability database; it actually looks at multiple, including Qualys's specific database, and provides you risk prioritization. That is one very fantastic feature that I enjoy with working with Qualys TotalCloud..”

MiracleChukwudebe

Cybersecurity Leader / Consultant at Ethnos IT Solutions

[Read full review](#) 

“Qualys TotalCloud is a one security platform where we could leverage the existing Qualys platform and not any other different agent or different platform for cloud visibility and cloud security. We had multi-cloud visibility where both AWS and Azure could be controlled and monitored for misconfigurations and security issues.

We had better integration with tools, which is where Qualys TotalCloud was useful.

TruRisk insights have been useful in helping us move from a traditional vulnerability counting approach to a risk-based approach. .”

Verified user

Senior security analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

In my experience, the best feature Qualys TotalCloud offers is the FlexScan feature, which delivers multi-modal asset discovery using agentless and agent-based network and pipeline scanning.

The FlexScan feature has benefited our environment because we recently found a vulnerability rated high to medium risk in our assets, which we were able to discover and fix using Qualys TotalCloud.

“Qualys TotalCloud positively impacts our organization by helping to minimize downtime in relation to asset scanning and by improving the overall cyber inputs in the enterprise.

“Since using Qualys TotalCloud, we have noticed faster remediation times and improved compliance because the single scanning dashboard allows us to see all our assets in multi-cloud as well as on-premises deployment, which helps the cyber team quickly remediate any open vulnerabilities across different assets. .”

Sanchit Makkar

[Read full review](#) 

Dns architect at a outsourcing company with 5,001-10,000 employees

“The best features Qualys TotalCloud offers are cloud asset visibility, vulnerability assessment, and risk prioritization. This risk-based prioritization helped me quickly identify high-risk vulnerabilities and focus on remediation instead of going through every finding. TrueRisk-based prioritization is useful for understanding which vulnerabilities need attention first.

“It improved our workflow mainly by giving us a single view of cloud assets and their risk, so we could focus on the higher priority vulnerabilities instead of reviewing every finding manually. This helped us prioritize remediations more efficiently and reduce the time spent on vulnerability assessment and follow-up.

“Qualys TotalCloud helped us identify exposures that might otherwise have been missed, especially across cloud assets, vulnerabilities, and identities. With the SaaS configuration, the unified inventory and risk view made it easier to connect vulnerabilities with asset criticality, exposure, and access permissions, allowing us to investigate high-risk exposures first and address them before they could become bigger security issues..”

Verified user

[Read full review](#) 

Soc Analyst at a manufacturing company with 10,001+ employees

“The best features Qualys TotalCloud offers currently include managing cloud infrastructure and container security while facing major challenges such as alert fatigue. Traditional vulnerability scanners flag hundreds of CVEs on short-lived Kubernetes containers, some of which have no internet exposure or are gone before we can even triage them. I leverage Qualys TotalCloud to move beyond static CVSS. I use it to implement runtime exposure, correlation risk reprioritization, and shift-left integration. This notifies developers to fix a base image upstream rather than patching live ephemeral instances.

“In my work with cloud and container security, the biggest operational hurdle was alert fatigue. I use Qualys to shift left from static CVSS severity to context-aware risk prioritization. I correlated raw vulnerability data with real-time risk factors such as public network exposure, active runtime execution, or overly permissive IAM roles. This allows us to immediately drop the priority of isolated containers and escalate lower-severity CVEs that sit on an exposed, high-risk path. We can map these findings directly back to our CI/CD pipelines so developers can patch the root base images upstream. We have drastically cut down the signal-to-noise ratio, saved a lot of manual hours doing triage work, and ensured engineering effort goes directly towards high-impact risk reduction..”

Verified user

[Read full review](#) 

Sr Security Engineer at a tech vendor with 5,001-10,000 employees

“Qualys TotalCloud offers several valuable features, including monitoring visibility as an EDR tool and cloud asset inventory capabilities, which help in centralized asset management and prioritizing risk.

“It is particularly useful because it gives us visibility across cloud resources from different environments in one place, making it easy for organizations to understand their security postures without manual checking with cloud consoles.

“The vulnerability management capabilities are another strong point where we can review security risks for vulnerabilities on cloud workloads and prioritize issues based on CVSS scores.

“When we were using different cloud solutions, it was tedious to find compliance for assets, especially during monthly meetings.

“Qualys TotalCloud is very useful in day-to-day security operations, particularly at monthly review meetings. It was helpful to maintain all the assets in one place, and when investigating vulnerabilities, we can first identify affected cloud assets from the inventory and look at their release details and security findings which helps in understanding the actual scope of an issue and identifying which team needs to take action.

“I believe it saves us more time because we do not have to gather asset information from different sources and tools. We can search and filter inventory, group assets, and use asset context to move quickly from understanding what an asset is to identifying required security patches.

“Qualys TotalCloud has positively impacted our organization by helping us save time and manage all assets and remediation, allowing us to achieve quarterly and half-yearly goals.

“It has improved our visibility and made vulnerability management more structured, helping us reach our remediation goals while reducing manual effort from security reporting and patch management.

“Before implementing Qualys TotalCloud, we used to have around ten thousand vulnerabilities on critical servers, and after using it, we reduced the vulnerabilities

by thirty to forty percent in just two months.

“We could identify vulnerabilities and their affected assets within five to ten minutes. This has also improved our investigation efficiency, allowing the team to spend more time on actual remediation rather than data collection..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

Other Solutions Considered

“I used a different solution previously, but I cannot disclose the name of it. Comparing it with TotalCloud, it allowed our team to shift from volume scanning to context-aware risk management. Qualys TotalCloud was a better solution for us..”

Verified user

Sr Security Engineer at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

“Apart from Tenable and Qualys, I did not work with any other competitors. I only worked with these two and OpenVAS, which is an open-source solution for vulnerability assessment..”

Mahmoud Younes

Cyber Security Architects at VaporVM

[Read full review](#) 

“For a mid-size bank like ours, the licensing cost for Qualys TotalCloud is cheap. Tenable Enterprise costs double that of Qualys TotalCloud and Rapid7. We explored those three solutions and decided to go with Qualys TotalCloud..”

Robert Orłowski

IT Security Expert at Alior Bank S.A.

[Read full review](#) 

“Right now, we are using Tenable, specifically Tenable Nessus, as our VAPT tool, and we are seeking different options, which is why we have started the evaluation for Qualys TotalCloud..”

NishantKandpal

Information Security Manager at Varun Beverages Ltd

[Read full review](#) 

“It is difficult to compare the helpfulness of written explanations with other solutions as we used Nessus for a few years. We only had two or three years of experience with that support, and it was simply Nessus Professional and not Tenable Enterprise, so I could not make a comparison. However, currently we have very good support from our integrator, plus the support from Qualys itself..”

Robert Orłowski

IT Security Expert at Alior Bank S.A.

[Read full review](#) 

“When looking at Qualys TotalCloud and Prisma Cloud, I believe Prisma does a better job with scanning for infrastructure as code, enabling organizations using the infrastructure as code cloud model to identify vulnerabilities even at the code level. Overall, Qualys TotalCloud is a good solution, and it is catching up. Initially, I knew Qualys as just an on-premises vulnerability management solution, but now they keep upgrading their features, solutions, and dashboards. They are working on minimizing alert fatigue and offering broader compliance coverage, though I believe their compliance coverage is somewhat limited. Currently, I cannot generate compliance reports for some specific frameworks relevant to my region, and if Qualys can enhance that, it will be a significant improvement..”

MiracleChukwudebe

[Read full review](#) 

Cybersecurity Leader / Consultant at Ethnos IT Solutions

ROI

Real user quotes about their ROI:

We have seen a return on investment since using Qualys TotalCloud, as we are able to scan all our assets with less human intervention and achieve overall effective outcomes.

Sanchit Makkar

[Read full review](#) 

Dns architect at a outsourcing company with 5,001-10,000 employees

“TotalCloud has yielded significant cost savings by reducing manual effort by 20 to 30 percent and generating overall savings of 30 to 40 percent across various departments..”

Verified user

[Read full review](#) 

Security Manager at a consultancy with 10,001+ employees

“I was not involved in the investment part of it, but I definitely know that it has delivered a high return on investment based on the drastically reduced triage labor and tool consolidation, rather than reducing the headcount outright..”

Verified user

[Read full review](#) 

Sr Security Engineer at a tech vendor with 5,001-10,000 employees

“I do not have any relevant metrics available, but I can definitely say Qualys TotalCloud has saved our time by giving us better asset visibility and risk-based prioritization, as it has reduced the time spent manually reviewing CVEs and deciding what to address first..”

Verified user

[Read full review](#) 

Soc Analyst at a manufacturing company with 10,001+ employees

“It saves a lot of time and manual effort. We have many options to raise a case if it can be automated. CallStream helps us integrate and automate tasks. It helps us automate lots of things..”

SurajTripathi

[Read full review](#) 

Senior Security Consultant at CyberNxt Solutions LLP

“It helps us because we have monthly meetings with our leadership team. These graphs help us give the return on investment of the product to the leadership team and also give us an overview of how this product is working, what the thresholds are, and how the configurations are working or not. This helps us determine that..”

Nadeem-Inamdar

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

[Read full review](#) 

Use Case

“Qualys TotalCloud helps with aggregating assets and provides visibility around cloud assets. It also helps with integrating internal on-premises assets, giving you that view. You are able to see vulnerabilities across cloud infrastructure, whether it is AWS or Azure. Qualys TotalCloud can correlate and give you a bird's-eye view of your cloud infrastructure or environment..”

MiracleChukwudebe

Cybersecurity Leader / Consultant at Ethnos IT Solutions

[Read full review](#) 

“I have been using Qualys TotalCloud for two years.

“My main use case for Qualys TotalCloud is vulnerability management.

“As a specific example of how I use Qualys TotalCloud for vulnerability management, it creates a Jira ticket for any vulnerability that it finds in our containers, as well as in any of our platforms and other cloud resources..”

Verified user

Sr Security Engineer at a tech vendor with 5,001-10,000 employees

[Read full review](#) 

I have been using Qualys TotalCloud for the last eight months to scan the hardware and the virtual devices in our infrastructure.

Our main use case for Qualys TotalCloud is to secure our multi-cloud environment containers and workloads across AWS, Azure, GCP, and OCI as a single control plane.

“Having a single control plane helps my team manage those multi-cloud environments more efficiently because it allows us to consolidate multiple cloud assets, configurations, and security postures into a single dashboard.

“We also use Qualys TotalCloud to automate remediation plans, which offers one-click fixes and workflows that automate the resolution of misconfigurations quickly. .”

Sanchit Makkar

Dns architect at a outsourcing company with 5,001-10,000 employees

[Read full review](#) 

“I mainly use Qualys TotalCloud for vulnerability management and cloud security to identify vulnerabilities in cloud assets, assess their severity, prioritize remediation, and track the overall security posture.

“When reviewing cloud assets for newly identified vulnerabilities, I check the vulnerability details and severity in Qualys TotalCloud, prioritize the high-risk findings, and share the remediation requirements with the relevant team while following up on progress.

“I found the visibility provided across cloud assets useful in Qualys TotalCloud as it made it easier to identify high-risk vulnerabilities, prioritize them based on severity, and track the remediation with the relevant teams.

“The AI governance and security capabilities of Qualys TotalCloud are useful, especially for visibility and risk control. From my experience, I primarily value having visibility into AI-related assets and configurations and being able to identify security or compliance risks. The risk-based approach also helped me prioritize the issues that needed attention first..”

Verified user

Soc Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

“I primarily use Qualys TotalCloud for Cloud Security Posture Management, vulnerability management, asset visibility, and continual monitoring of cloud assets, maintaining the cloud resources that we use.

“One of the main advantages for us is having multiple security capabilities available through this tool, instead of maintaining several completely separate tools for each one of them, such as vulnerability management, audit asset visibility, and cloud security management.

“During our security rehearsal or weekly customer meetings, we need to check about site compliance, and Qualys TotalCloud was very helpful because instead of using other tools where we had to pull reports from different sources, we could check compliance all in one place.

“When one hundred fifty vulnerabilities were identified on cloud, production, or any endpoint, it was useful for us to identify which asset was affected and to look at the details and share the findings with the customer and the remediation infrastructure team..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“My main use case for Qualys TotalCloud is regarding the cloud visibility that we were not having previously.

Previously, we were just looking at critical vulnerabilities and patching them. Now with Qualys TotalCloud, we can distinguish between critical vulnerabilities and what is internet-facing, what is a sensitive workload, and excessive permissions that are given to unauthorized users in the cloud environment. This gives us more visibility towards what is happening in the cloud.

Another use case I have for Qualys TotalCloud is identifying misconfigurations within the cloud environment and how any configurations might impact the organization's cloud assets. Those were the two main use cases.

The integration with Qualys TotalCloud worked very well with tools such as Exonius and Splunk, wherein we were easily getting automated alerts and incidents that we could automate into emails and reach out to stakeholders without manual intervention.

Qualys TotalCloud is definitely helpful for our vulnerability management. It did help in CSPM and also in looking at cloud inventory, not just when a vulnerability or misconfiguration is happening, but I could look at what is happening in my cloud environment, who is really having any entitlements, what access exists, what unauthorized access anyone has, and so on.

Qualys TotalCloud does provide both IaaS and SaaS when it comes to threat assessment.

EASM finds assets that are exposed to the internet such as domains, IPs, applications, and services. When it comes to SaaS, it assesses the SaaS applications and their security posture. We could also look at what SaaS services we are using and what risks they introduce.

We were narrowing the risk and threat down to a much smaller group of assets where multiple factors came together. For example, a highly vulnerable asset that

was internet-facing and business-critical had additional exposure of configuration issues. We used those insights to prioritize the assets for immediate remediation.

.”

Verified user

Senior security analyst at a manufacturing company with 10,001+ 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.

“Our experience with the setup and deployment was quite good; Qualys was supportive, and we met with them twice a week while setting up the scanners and operations..”

Verified user

[Read full review](#) 

Senior Technical Program /Product Manager at a transportation company with 10,001+ employees

“I was not involved in pricing, setup cost, and licensing, but I can say that the setup was fast, within a quarter, and it scales well with a stable infrastructure. I think it is highly dynamic..”

Verified user

[Read full review](#) 

Sr Security Engineer at a tech vendor with 5,001-10,000 employees

“In terms of installation, it could be simplified compared to other tools due to its packaging and tooling. A lack of specific help articles and integration issues are present. From a security standpoint, it is good but requires time..”

Verified user

[Read full review](#) 

Systems Engineer at a financial services firm with 10,001+ employees

“I recommend starting with a clear asset and inventory and properly configuring the cloud connector first. Once the environment is visible, it is important to spend time understanding TrueRisk prioritization instead of treating every severe finding equally. The initial setup and tuning of connectors, permissions, and policies is also important..”

Verified user

[Read full review](#) 

Soc Analyst at a manufacturing company with 10,001+ employees

“The deployment was not easy, but with the help of the support team, we completed it.

It took about a week because we had many accounts we needed to migrate, and we needed to check the policies and define our policies. It took time because everything cannot go in one go, so we did it in a phase-wise manner..”

Nadeem-Inamdar

[Read full review](#) 

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

“Regarding deployment of Qualys TotalCloud, the installation of Cloud agents was given to administrators from each team who manage servers and workstations, including components in Azure or GCP cloud. This was not handled by me or my team, as I work in the cybersecurity department. We manage the use of Qualys TotalCloud, but installation is up to the administrators, and we provide them support.

“Currently, in the cybersecurity department, we have two people involved in the deployment of Qualys TotalCloud, along with over one hundred administrators involved in implementing and installing agents on the machines..”

Robert Orłowski

[Read full review](#) 

IT Security Expert at Alior Bank S.A.

Customer Service and Support

“Customer support with Qualys TotalCloud needs a little improvement with the response times. Other than that, they are technically capable, but occasionally they are slow on low-tier tickets..”

Verified user

[Read full review](#) 

Sr Security Engineer at a tech vendor with 5,001-10,000 employees

“Regarding Qualys TotalCloud's AI capabilities, I do see that it is not true AI. It feels to me that I am working with a chat that does not give insights based on the findings or the information that I get from the tool. It is not a real agentic AI. It is more a chatbot..”

Verified user

[Read full review](#) 

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

“I rate the technical support from Qualys TotalCloud a perfect ten out of ten because whenever we log incidents, all service level agreements are met within half an hour, with prompt provision of root cause analyses by the support teams..”

Sourav Dadhwal

[Read full review](#) 

Cyber Expert at National Electronic Register Of Jain Manuscripts

“The support from Qualys TotalCloud is a ten out of ten. The support team is very helpful in every aspect. If we get any issues, we can directly communicate with them. They have been helpful from day one. They have been solving issues efficiently..”

Verified user

[Read full review](#) 

Cyber Security Specialist at a financial services firm with 10,001+ employees

“From a technical support perspective, those individuals are competent enough to provide information regarding the product. They offer level one support initially, escalating as needed. I rate them four out of five because they respond quickly if issues are marked as high priority. I would give them 8.5..”

Verified user

[Read full review](#) 

Systems Engineer at a financial services firm with 10,001+ employees

“Regarding technical support from Qualys, they respond, but the response time can be too long. Sometimes we need to wait weeks for solutions to simple questions.

“If I had to rate Qualys support based on my experience from one to ten, I would say around six or weak seven, perhaps six plus..”

Robert Orłowski

IT Security Expert at Alior Bank S.A.

[Read full review](#) 

Other Advice

“I have Qualys TotalCloud deployed in a hybrid model, running it mostly on-premises but also integrating cloud assets. I would definitely recommend Qualys TotalCloud. Qualys keeps improving and is one platform that continually tests and enhances its offerings. They are doing really well. I give this review a rating of 8..”

MiracleChukwudebe

Cybersecurity Leader / Consultant at Ethnos IT Solutions

[Read full review](#) 

“Most recommendations and findings are accurate and reliable. While the AI output is helpful, it is crucial to validate actions against actual safety configurations, as human intelligence is still necessary in decision-making.

“My advice for others considering using Qualys TotalCloud is that if you want all vulnerability management and cloud asset management in one place, then it is the best solution. Good configuration makes finding vulnerabilities and managing alerts much easier.

“My overall rating for this product is nine out of ten..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“I would give Qualys TotalCloud an eight out of ten rating. The remaining two points I would take out due to the improvements I have mentioned.

The biggest strengths of Qualys TotalCloud are that it is pretty good at cloud visibility, has easy integration, and also has multi-cloud compatibility.

I would probably do a traditional CVE-based approach otherwise. A large number of vulnerabilities can be classified as critical or high, but treating all of them with the same priority is not practical.

Qualys TotalCloud compares well because it combines breadth and integration. I am pretty sure VMDR gives strong vulnerability visibility. But when we want visibility for the cloud environment, that is where Qualys TotalCloud comes into the picture. The biggest advantage is correlating the findings that we receive from these security tools and through the risk prioritization and managing the entire cloud ecosystem..”

Verified user

Senior security analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

“I found the overall asset visibility with the unified risk view useful, as having vulnerabilities, cloud assets, and risk context in one place made investigation easier and reduced the need to switch between different tools.

“It has helped me focus on the vulnerabilities that actually needed attention instead of treating every finding equally, as I used the risk score and asset context to identify higher risk issues first, making it easier to prioritize remediation and reduce the time spent manually reviewing lower risk findings.

“I found the output generally reliable for identifying and prioritizing security risks, as the results were useful for deciding which findings needed attention first, although I would still validate the important findings before taking any remediation actions.

“It helped identify a smaller set of assets with higher TrueRisk scores. I use that

information to prioritize those assets for further investigation, review the vulnerabilities and exposures contributing to the score, and coordinate remediation with the relevant teams. This helped us focus on the assets with higher potential impact instead of treating all vulnerabilities equally.

“TrueRisk helps reduce the noise from raw CVEs by putting them into business and threat context. Instead of treating every high severity CVE equally, we could focus on vulnerabilities that were actually more likely to be exploited or affect important assets, which made prioritization and remediation much more efficient.

“Overall, I have a positive impression of the combination of detection and protection features in Qualys TotalCloud. The main advantage for me is having vulnerability assessment, cloud posture monitoring, and risk prioritization in one platform. Compared with more point-focused solutions, Qualys TotalCloud gives us a more unified view which makes it easier to prioritize risks and decide what needs attention first. I rate this review a 10 out of 10..”

Verified user

Soc Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

Regarding Qualys TotalCloud's AI capabilities, I have not noticed any reliability issues or anything worth mentioning; it is overall the best tool available in the market for scanning purposes.

Qualys TotalCloud is deployed on-premises in our physical data centers.

“Qualys TotalCloud provides unified vulnerability and threat assessment across both [IaaS](#) and SaaS, and this unified view has helped our overall cloud security posture management by reducing false positives in our scanning results. Qualys has made the scanning and performance of all assets quite effective.

“The TrueRisk Insights feature has helped in unified risk prioritization by consolidating vulnerabilities, misconfigurations, and threat intelligence into a single risk score, allowing our team to fix critical issues first.

“I assess the comprehensiveness of FlexScan in providing visibility across our on-premises, multi-cloud, and container environments as excellent because it allows our organization to combine agentless scanning for quick setup with agent-based scanning for deep continuous operating system inspections.

“Qualys TotalCloud has helped my team identify hidden cloud, runtime, data, identity, SaaS, application, or Shadow AI exposures before they became exploitable risks by providing a single control plane that reduces the need for separate security tools for different cloud vendors.

“We are using Qualys TotalCloud's flexible scanning options, specifically agent-based scanning, to improve coverage across long-lived and ephemeral cloud workloads.

“My advice for others looking into using Qualys TotalCloud is to be vigilant about the vulnerabilities that emerge and to have a remediation plan in place, as Qualys TotalCloud may trigger a lot of risks and vulnerabilities across many different assets in a multi-cloud environment. I provide this product with a rating of nine out of ten. .”

Sanchit Makkar

Dns architect at a outsourcing company with 5,001-10,000 employees

[Read full review](#) 

“My overall impression of the combination of detection and protection features in Qualys TotalCloud is that we were using another vulnerability management tool. The reason we changed was because Qualys has risk prioritization, CVE depth, and unified patch management. It is excellent at cutting down on false positives using runtime network context, and it focuses on pipeline prevention and guided workflow remediation.

“TruRisk has fundamentally shifted our cloud security from reactive vulnerability management to targeted, business-context risk reduction. Instead of just flagging an isolated CVE, TruRisk tells us a narrative, such as, "This isn't just a CVSS flaw; it

is a publicly accessible virtual machine running an actively exploited vulnerability with root privileges." TruRisk insights isolate 2% to 3% of workloads.

"Using TruRisk to mitigate noise from raw CVEs has transformed our vulnerability management, shifting teams away from basic CVSS scores and toward risk-driven reduction. In practice, relying strictly on CVSS results in an overwhelming alert volume, with 40% to 50% of the environment labeled as critical. TruRisk typically reduces the actionable queue to the top 2% to 5% of assets that pose a real operational danger.

"FlexScan has strong, multi-layered visibility across diverse environments by letting us blend agentless and agent-based assessment methods into a single view. Its overall comprehensiveness varies slightly depending on the specific tier of my stack. For us, it is mostly the container and Kubernetes environment, and the visibility is in-depth. Combining eBPF sensor technology allows for deep execution monitoring inside Kubernetes pods and hosts. It also scans container images, registries, and infrastructure as code before deployment, catching flaws upstream.

"Qualys TotalCloud provides unified vulnerability and threat assessment across both [IaaS](#) and SaaS environments. This is achieved by CSPM, CWP, and SSPM for a unified engine. For example, in [IaaS](#), an [S3](#) bucket or a [GCP](#) storage account might be restricted to internal access. However, if a user lacks MFA or has compromised credentials with wide-ranging read access to both SaaS and cloud infrastructure, TotalCloud will flag this combination as a risk factor. Seeing identity and infrastructure together prevents attackers from abusing over-privileged SaaS accounts to pivot to IaaS assets.

"Automating the risk-based triage with Qualys TotalCloud has freed up significant engineering bandwidth every week. This lets the team focus on proactive security architecture, platform automation, and strategic initiatives rather than manual ticket triage. There were around 10,000 tickets, but we are now able to track them sooner and faster and assign them to the correct teams to fix.

"Once it is set up, Qualys has proved to be one of our greatest assets. I rate this product an overall 8 out of 10.."

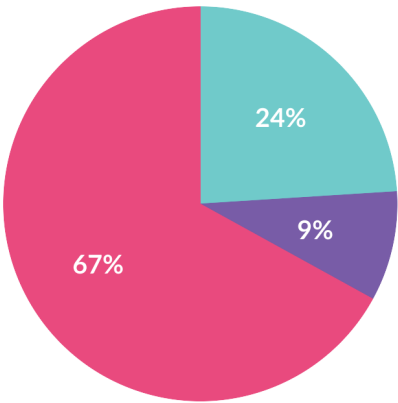
Top Industries

by visitors reading reviews

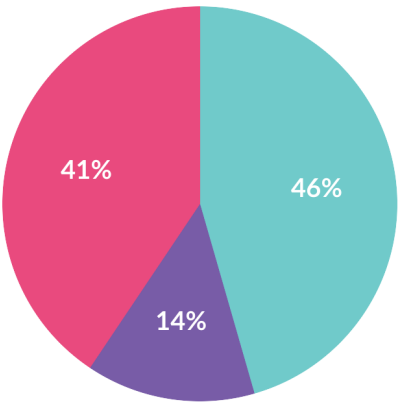


Company Size

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