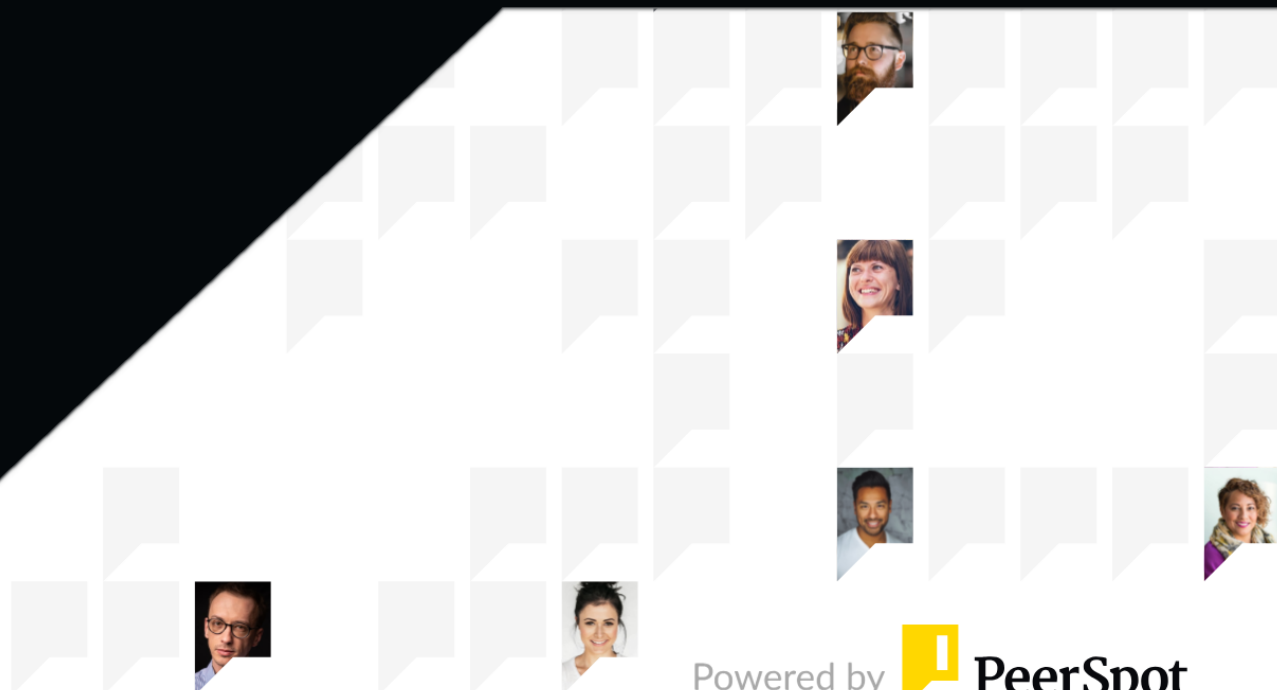




Qualys Exposure Management

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 - 23

Setup..... 24 - 26

Customer Service and Support..... 27 - 29

Other Advice..... 30 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

Product Recap



Qualys Exposure Management

Qualys Exposure Management Recap

Qualys VMDR is a comprehensive cybersecurity tool offering vulnerability management, patch management, and continuous monitoring with real-time asset discovery. It delivers scalable, cloud-based solutions that enhance security operations without additional infrastructure.

Qualys VMDR provides a robust platform for enterprise security, integrating vulnerability management, compliance, and asset inventory for full visibility across cloud and on-premises environments. It features a comprehensive dashboard with threat intelligence-driven prioritization and remediation capabilities. Users benefit from accurate assessments via agent-based scanning and appreciate the intuitive, customizable scanning and reporting interface. However, there's room for improvement in false positive reduction, UI simplification, and integration capabilities, along with enhancements in asset management for large-scale deployments and the vulnerability database. Enhancing technical support speed, patch management, compliance standards, and inter-module navigation would further enrich user experience.

What are the key features of Qualys VMDR?

- **Vulnerability Management:** Identifies and manages security vulnerabilities across environments.
- **Patch Management:** Ensures systems are updated with the latest patches.
- **Continuous Monitoring:** Offers real-time insights into security posture.
- **Asset Discovery:** Provides up-to-date asset inventory and visibility.
- **Threat Intelligence:** Enhances prioritization and remediation processes.
- **Customizable Dashboard:** Facilitates easier scanning and reporting through an intuitive interface.

What benefits can users expect when evaluating Qualys VMDR?

- **Scalability:** Cloud-based deployment offers easy, cost-effective expansion.
- **Accurate Assessment:** Agent-based scanning keeps security data current.
- **Enhanced Security Operations:** Comprehensive features streamline vulnerability management.
- **Advanced Reporting:** Facilitates detailed insights for better security decision-making.

Qualys VMDR is widely used in industries needing stringent security and compliance measures, offering comprehensive vulnerability and compliance management. It is deployed to secure web applications, servers, and crucial assets, supporting a wide range of sectors by ensuring policy adherence and vulnerability tracking through its powerful cloud platform.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “For vulnerability management, Qualys Enterprise TruRisk Management is very good for our organization.”



Ajay Paul

System Engineer at a outsourcing company with 10,001+ employees

- ✓ “Qualys Enterprise TruRisk Management is a very good software application to scan each and every vulnerability and, through that, it prevents the attackers from exploiting the systems, servers, or our data and prevents data leaks in short.”



Roshan Ugale

Junior Associate at ESDS Software Solution Pvt Ltd.

- ✓ “Regarding its competitors in the market, I believe Qualys Enterprise TruRisk Management has a strong offering.”



Pramod Borana

Senior Manager at a financial services firm with 10,001+ employees



“Risk-based prioritization is a new feature with Qualys Enterprise TruRisk Management, and overall, the vulnerability posture of our organization has improved significantly.”



SharmaAbhijeet

Senior Project Engineer at CDACINDIA



“The initial setup and onboarding process of Qualys VMDR was quite smooth, as we were able to draft the SOPs from the documentation portal itself and everything was available in the documentation, so it was not a hassle for us to get the integrations done on time.”



Vaibhav Ghule

Soc Lead & Edr Administration at Persistent Systems



“Qualys is a very good tool for companies, and the different tools this brand offers bring all the necessary tools for good development for these companies.”



LuisPerez11

QA Manager at a consultancy with 51-200 employees



“Qualys VMDR has positively impacted my organization by reducing vulnerability exposure time through faster detection and patching, and it has improved compliance reporting with accurate and up-to-date data.”



Verified user

Cyber Security Solution Engineer at a computer software company with 201-500 employees

What users had to say about valuable features:

“The most valuable feature is the ability to get vulnerability lists for bulk systems. My company has more than 300,000 employees, so we can generate a report of all systems and filter the results by location. This is the most interesting aspect of the tool. Additionally, Qualys Enterprise TruRisk Management provides many scoring metrics for critical and non-critical vulnerabilities, as well as high-risk ratings. This allows us to prioritize which vulnerabilities are more critical and focus on those first. Qualys Enterprise TruRisk Management also provides resolutions for vulnerabilities. For example, if a Windows update is missing, we can patch those systems directly from Qualys Enterprise TruRisk Management. It will connect directly to the Microsoft site and download the patch, so there is no need to search for patches separately. The patch will install directly from Qualys Enterprise TruRisk Management itself. For vulnerability management, Qualys Enterprise TruRisk Management is very good for our organization..”

Ajay Paul

System Engineer at a outsourcing company with 10,001+ employees

[Read full review](#)

“The best features of Qualys Enterprise TruRisk Management are the capability to search and mitigate vulnerabilities from attackers in endpoints and focus on the preventive view of organizational security through virtual patching, making this function automatic for cybersecurity teams.

“Qualys is a very good tool for companies, and the different tools this brand offers bring all the necessary tools for good development for these companies. Once it is set up, it works well.

“Qualys has a new tool called Total AI, which requires review of the use and correct use of AI in companies and review and protection of the information that collaborators use in AI..”

LuisPerez11

QA Manager at a consultancy with 51-200 employees

[Read full review](#) 

“The most valuable function of Qualys Enterprise TruRisk Management is that it provides a clear picture of how my vulnerabilities across different servers can be categorized. I must provide input about servers and their criticality, but based on that information, it gives me a clear understanding of whether a particular vulnerability on my server needs to be fixed based on the proof of concept and attack vectors available in the market. Based on this, it provides me a scoring mechanism that tells me which vulnerabilities I need to patch immediately or which ones I can defer for a later time.

“Qualys Enterprise TruRisk Management provides me with a QDS scoring mechanism, which has helped me identify which vulnerabilities I need to patch immediately. It also provides me with the criticality rating of each vulnerability. Understanding whether a vulnerability needs immediate action or whether I can take some time based on my current posture and available bandwidth has been instrumental..”

Pramod Borana

Senior Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“From what I have seen and communicated with my team, True Risk is something that highlights separately. True Risk identifies which vulnerability needs patching, not solely based on the CVSS score. There could be vulnerabilities with higher CVSS scores, but it is not necessary to patch them on a priority basis. There could be others that need remediation despite having low CVSS scores. The prioritization from True Risk is what I appreciate the most.

“Qualys VMDR's continuous monitoring capabilities help us respond to emergent threats by enabling my team to reach out to the security engineers whenever there is any detection of a vulnerability, informing them about it, and creating an incident. We work through the incident response phases. We identify the vulnerability and take necessary decisions on whether we need to patch or update software on which vulnerabilities are identified. If there are vulnerabilities regarding open ports or open services, we decide to block the exposed ports..”

Vaibhav Ghule

Soc Lead & Edr Administration at Persistent Systems

[Read full review](#) 

“Qualys Enterprise TruRisk Management is quite good for analyzing and scanning the systems individually. It not only scans the system but also shows the hardware vulnerability as well. If there is any low hardware, for example, if there is one application running on DDR3 RAM, and the same application running on DDR4 RAM, it will show that this application will perform better on DDR4. It will be good or best to change your hardware. These kinds of things Qualys Enterprise TruRisk Management shows to us. For our infrastructure, it helps us understand how we can run our infrastructure smoothly without preventing any downtime. It also shows the remedies, such as how we can close those vulnerabilities, bugs, and loopholes if we find in our systems and infrastructure on our servers. It scans each and everything deeply. For example, if you just created a text file and you keep that file for one year, it will show you that file name, file path, and it will reflect as a vulnerability. It shows why this file was just left in your system for the last one year. Qualys Enterprise TruRisk Management is a very good software application to scan each and every vulnerability. Through that, it prevents the attackers from exploiting the systems, servers, or our data. It prevents data leaks in short..”

Roshan Ugale

Junior Associate at ESDS Software Solution Pvt Ltd.

[Read full review](#) 

“Qualys Enterprise TruRisk Management is a centralized vulnerability platform that provides us with wide centralized visibility. It has risk-based prioritization, useful reporting capabilities, and integration with different assets is quite easy. It is scalable in our environment.

“With Qualys Enterprise TruRisk Management, we are able to perform risk-based prioritization. It is scalable for our environment, which gives us a good advantage. Reporting is very useful, so we get valuable reports.

“Risk-based prioritization is a new feature with Qualys Enterprise TruRisk Management, and overall, the vulnerability posture of our organization has improved significantly. Qualys has quite improved the overall vulnerability management.

“With Qualys Enterprise TruRisk Management, we are able to automate processes and prioritize risks. The resources who were previously working on the administrative part of vulnerability management are now free to work on different areas and are able to automate the administrative part. They are working on the automation and are able to address different vulnerabilities and patch them in time. This helps us considerably, and resources are easily managed.

“With Qualys Enterprise TruRisk Management, all three metrics have improved. Resource allocation has decreased, time has improved, and we are getting positive results..”

SharmaAbhijeet

Senior Project Engineer at CDACINDIA

[Read full review](#) 

Other Solutions Considered

“The main differences between Tenable and Qualys is the model that brands use to consume the product; the licensing or size is different between Tenable and Qualys..”

LuisPerez11

QA Manager at a consultancy with 51-200 employees

[Read full review](#) 

“I have not used other solutions in this company. However, in my previous company, I used a tool called ManageEngine. Compared with ManageEngine, Qualys Enterprise TruRisk Management is by far better..”

Ajay Paul

System Engineer at a outsourcing company with 10,001+ employees

[Read full review](#) 

“I have experience with competitors including Tenable, Nessus, and Rapid7. To be honest, they ask a high price, but they also provide certain functionality that other competitors do not. In the market, if you are pricing higher, that is what you can expect..”

Pramod Borana

Senior Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“Before choosing Qualys Enterprise TruRisk Management, we conducted a requirement analysis and selected a few vendors. We performed our own proofs of concept and finalized Qualys..”

SharmaAbhijeet

Senior Project Engineer at CDACINDIA

[Read full review](#) 

“We were using a ManageEngine solution previously with Qualys Enterprise TruRisk Management, and we were conducting a proof of concept. As our environment was quite large, we migrated to Qualys, which proved to be more useful and more powerful for this environment..”

SharmaAbhijeet

Senior Project Engineer at CDACINDIA

[Read full review](#) 

“As a product and solution, Qualys Enterprise TruRisk Management is one of the best I have ever seen. Another solution I would mention is BigFix. BigFix is quite popular, and I would place that one in the first position and Qualys Enterprise TruRisk Management in the second position. Regarding the rating, Qualys Enterprise TruRisk Management is also better, but most of the features and things are more in BigFix. According to me, I would give eight out of ten for Qualys Enterprise TruRisk Management for all its features..”

Roshan Ugale

Junior Associate at ESDS Software Solution Pvt Ltd.

[Read full review](#) 

ROI

Real user quotes about their ROI:

“Qualys VMDR helps us be compliant, and vulnerability management is a crucial part of maintaining our organization's security, significantly contributing to ROI..”

Verified user

Works at a comms service provider with 1-10 employees

[Read full review](#) 

“We saw a return on investment through significant savings in time, money, and resources. The solution allowed for efficient task management among team members..”

Shubhajit Saha

System Admin at a tech services company with 10,001+ employees

[Read full review](#) 

“Qualys provides good value for the investment. Before using Qualys, we weren’t clear on how many assets needed purging or how many open vulnerabilities we had. Qualys gave us a clearer picture, so from a cost perspective, it’s been valuable..”

Lakshay Grover

Works at a tech consulting company with 10,001+ employees

[Read full review](#) 

“We have seen a significant ROI with Qualys, which is estimated to be around twenty to thirty percent. It has saved a lot of time and money by allowing us to mitigate issues without user interaction and preventing breaches..”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“Within three months of deployment, we began seeing improvements in vulnerability management. This helped us significantly reduce vulnerabilities and streamline our patch management processes, providing a notable return on investment..”

Koketso Ditlhage

Information Communication Technology Specialist at UNIVERSITY OF JOHANNESBURG

[Read full review](#) 

“I can see the time-to-value benefits of Qualys. It's more of a time and resource. Security is always an expense. We don't get active revenue out of it, so it's more of an expense.

So returns in terms of risk reduction. It helps us to identify those potential vulnerabilities on time and help facilitate those. So in those terms, it's a return on investment.

It saved us 20% of time because it is easy to use, and since it is integrated, we don't have to touch anything much. .”

MohitGupta2

Chief Information Security Officer Teleperformance India And Global Business Services at a financial services firm with 10,001+ employees

[Read full review](#) 

Use Case

“When a company needs to review and focus on all the vulnerabilities for their endpoints from actualizations or patches and all the programs they have installed, they need actualizations or to have this function available regarding the main use cases for Qualys Enterprise TruRisk Management..”

LuisPerez11

QA Manager at a consultancy with 51-200 employees

[Read full review](#) 

“I use Qualys Enterprise TruRisk Management for vulnerability management. We receive reports daily from Qualys Enterprise TruRisk Management that show which systems have vulnerabilities and prioritize them based on risk factors. This allows us to identify which systems have more vulnerabilities or higher risk levels and take appropriate action. We primarily use this tool for patch management and vulnerability patch management..”

Ajay Paul

System Engineer at a outsourcing company with 10,001+ employees

[Read full review](#) 

“We are using Qualys Enterprise TruRisk Management for vulnerability management. It identifies, prioritizes, and remediates vulnerabilities while focusing on the business risk itself. The latest TruRisk platform provides this functionality, and we are not just getting vulnerability counts, but we are actually working on the business risk of the vulnerabilities.

“We automate the vulnerability patching with Qualys Enterprise TruRisk Management and use patch management as well. In this overall scenario, we are automating the risk factor using Qualys for risk..”

SharmaAbhijeet

Senior Project Engineer at CDACINDIA

[Read full review](#) 

“Primarily, I use Qualys Enterprise TruRisk Management for assessing the current posture of my infrastructure as I am responsible for vulnerability management for my organization. Qualys Enterprise TruRisk Management gives me a clear picture of the current status of vulnerabilities relative to different criteria across my various integrated servers.

“I work in a regulated banking entity, so we are highly regulated. Most of our data comes from Qualys itself, making all data auditable from the standpoint of Indian regulators. Every data point that comes out of Qualys is auditable.

“I work with Qualys Enterprise TruRisk Management, though we are not using Patch Management. Beyond that, we are using Vulnerability Management and Secure Configuration, which is the new name for Policy Audit in Qualys..”

Pramod Borana

Senior Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“I mostly work on Qualys Enterprise TruRisk Management. I work in an organization where I use cybersecurity to address cyber threats and system vulnerabilities. We focus on keeping the systems away from attackers, ensuring the system stays up to date and healthy, and increasing the performance of the system. For that purpose, we use Qualys Enterprise TruRisk Management.

“Qualys has multiple products, and the particular product we use is Qualys Enterprise TruRisk Management. As per your need, if you want to use Qualys Enterprise TruRisk Management for the assessment of vulnerabilities and only scanning, we use Qualys software for scanning the systems, taking out the report, taking out the remedies, and taking out the severity and compliances for these things. If someone wants to understand what purpose exactly they want to use Qualys Enterprise TruRisk Management for, it would be better to evaluate their needs. There are seven to eight other similar tools to Qualys Enterprise TruRisk Management, such as cybersecurity asset management, TruRisk management, vulnerability management, detection, and response. If they want to only take out the report for vulnerability management, detection, and response, that tool will be better. If they want compliance reports, remedies reports, severity reports, and everything that will impact their infrastructure, then Qualys Enterprise TruRisk Management will be better. Additionally, we can push the patch from Qualys Enterprise TruRisk Management to a particular system or server. If someone wants all things handled only by Qualys Enterprise TruRisk Management, they can go with the advanced version..”

Roshan Ugale

Junior Associate at ESDS Software Solution Pvt Ltd.

[Read full review](#) 

“In my role, I work with Qualys VMDR as part of my responsibilities managing security operations and SecOps. I am currently a CrowdStrike administrator focused on EDR management, while my colleague serves as the Qualys administrator. Along with my responsibilities as a CrowdStrike administrator and EDR admin, I also serve as SOC Lead for the Security Operation Center. In this capacity, I need to navigate through all the tools in our security architecture to obtain details about any incidents or vulnerabilities that are detected. To accomplish this, I navigate through the CSAM and VMDR to check which devices have vulnerabilities present and how they are prioritized. I also check these details through True Risk in Qualys. These are the tools and features I navigate in the Qualys VMDR dashboard or portal when I log in.

“For my team, they have the use cases and necessary information readily available. Using Qualys VMDR is primarily to obtain vulnerabilities on the assets we have. Once they prioritize the vulnerabilities, I connect them with the MDM admins, which is InTune or JAMF. For Mac systems, we use JAMF, and for Windows systems, we use InTune. I function as a mediator between my Qualys team and the MDM team to get things done.

“We have been using the asset tagging and reporting features in Qualys VMDR. Qualys VMDR's continuous monitoring capabilities help us respond to emergent threats by enabling my team to reach out to the security engineers whenever there is any detection of a vulnerability, informing them about it, and creating an incident. We also work through the incident response phases. We identify the vulnerability and take necessary decisions on whether we need to patch or update software on which vulnerabilities are identified. If there are vulnerabilities regarding open ports or open services, we decide to block the exposed ports.

“The initial setup and onboarding process of Qualys VMDR was quite smooth. We were able to draft the SOPs from the documentation portal itself. Everything is available in the documentation, so it was not a hassle for us to get the integrations done on time..”

Vaibhav Ghule

Soc Lead & Edr Administration at Persistent Systems

[Read full review](#) 

Setup

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

“The initial setup and onboarding process of Qualys VMDR was quite smooth. We were able to draft the SOPs from the documentation portal itself. Everything is available in the documentation, so it was not a hassle for us to get the integrations done on time..”

Vaibhav Ghule

Soc Lead & Edr Administration at Persistent Systems

[Read full review](#) 

“The setup is straightforward and easy. We deployed scanners and agents on all our devices, configured the network, whitelisted policy scanners, and public URLs. Testing was conducted before deploying, and it went smoothly..”

Verified user

Works at a comms service provider with 1-10 employees

[Read full review](#) 

“Although I was not present during the initial deployment process, it's pretty straightforward. It's just an agent installation, which automatically connects it to the cloud platform, so the implementation won't take as long..”

Verified user

[Read full review](#) 

Security Engineer at a consultancy with 10,001+ employees

“The initial setup of Qualys VMDR was easy. We just had to open the Qualys tool, add the IP addresses of the respective servers or hostnames, and start scanning. Access to vulnerability assessment is only provided via IP addresses, not hostnames..”

VIKAS KUMAR YADAV

[Read full review](#) 

Solutions Architect at a consultancy with 10,001+ employees

“My experience with pricing, setup cost, and licensing shows that we can consider both time and money saved.

“The detail I can share is that it is around 30 to 40%..”

Verified user

[Read full review](#) 

Cyber Security Solution Engineer at a computer software company with 201-500 employees

“Overall, the initial setup for Qualys Enterprise TruRisk Management is good and straightforward. I have taken the SaaS model and am not discussing the on-premises model. I am working with the SaaS model. Scanners and QGS need to be deployed on-premises, which is straightforward. I only need to build a server and deploy the ISO. Qualys provides the SaaS model itself. Overall, if I go with the SaaS model, I would not find much difficulty or hindrance..”

Pramod Borana

[Read full review](#) 

Senior Manager at a financial services firm with 10,001+ employees

Customer Service and Support

“I cannot contact Qualys Enterprise TruRisk Management directly. Only our Qualys team can contact them. I do not have the ability to contact them directly..”

Ajay Paul

System Engineer at a outsourcing company with 10,001+ employees

[Read full review](#) 

“We reach out to customer support for Qualys Enterprise TruRisk Management occasionally, and it is quite easy to reach them. False positives are the main issue that we encounter and need to be handled by the support team..”

SharmaAbhijeet

Senior Project Engineer at CDACINDIA

[Read full review](#) 

“The support has not been very responsive, and we are receiving RCAs a little delayed whenever we raise support cases or communicate with the TAMs. I would rate the tech support of Qualys a six because of the unsatisfactory experience we have experienced..”

Vaibhav Ghule

Soc Lead & Edr Administration at Persistent Systems

[Read full review](#) 

“We have already done technical support for Qualys Enterprise TruRisk Management so many times. Since we use it daily, I know much more than the Qualys Enterprise TruRisk Management technical supporter sometimes in some things. I would give out of ten around seven out of ten..”

Roshan Ugale

Junior Associate at ESDS Software Solution Pvt Ltd.

[Read full review](#) 

“In the brand I work for, we have a very good team of many engineers who are prepared and certified with the levels of support for these tools from this brand, which helps me evaluate the customer service from Qualys or their technical support.

“The level of support is a nine out of ten.

“They provide very good support..”

LuisPerez11

QA Manager at a consultancy with 51-200 employees

[Read full review](#) 

“Regarding pricing, Qualys Enterprise TruRisk Management is a more costly product compared to what is available in the market. However, it does provide good features that justify the investment. My competitors, including Tenable, Rapid7, and other products, do not provide a good GUI function where I can actively track my vulnerabilities in real time. I always need to pull down a report in Excel and then work with the Excel file. With Qualys Enterprise TruRisk Management, I can work directly on the dashboard itself and ensure that all my servers are scanned within twenty-four hours or four hours according to my feasibility. Regarding its competitors in the market, I believe Qualys Enterprise TruRisk Management has a strong offering.

“The GUI in Qualys Enterprise TruRisk Management is excellent. Although it is quite elaborate and may require some navigation, it is very familiar and easy to use. Compared to other solutions, the GUI is superior..”

Pramod Borana

[Read full review](#) 

Senior Manager at a financial services firm with 10,001+ employees

Other Advice

“Qualys Enterprise TruRisk Management is very easy to use. If we have access to the system, there is no need for high technical knowledge, and an average person can navigate and use this tool easily. The tool is also available as a web application, making it very easy to access. If we have internet connectivity and a password, we can access it from any laptop or location. The entire process depends on the type of vulnerability being addressed. For example, for Windows patch updates, the process takes between half an hour and one hour to fully complete, depending on internet speed. I consider this a normal timeframe and it does not take excessively long. I would rate this review an 8.5 out of 10..”

Ajay Paul

System Engineer at a outsourcing company with 10,001+ employees

[Read full review](#) 

“We reach out to customer support for Qualys Enterprise TruRisk Management occasionally, and it is quite easy to reach them. False positives are the main issue that we encounter and need to be handled by the support team.

“If you are looking for a good vulnerability management platform with Qualys Enterprise TruRisk Management and are open to a cloud-based or hybrid-based environment with good scalability for a large environment, you should choose Qualys. I would rate this solution a 9 out of 10..”

SharmaAbhijeet

Senior Project Engineer at CDACINDIA

[Read full review](#) 

“Agentic AI is one of the models running in the background for Qualys. It is responsible for all vulnerability closures and vulnerability testing. All data collected by agents in the field is gathered and pushed into the Agentic AI model, which then processes that information and provides output based on proof of concept mechanisms or the MITRE ATT&CK pattern.

“Based on my understanding, I have not found any false positives in Qualys Enterprise TruRisk Management. There are some vulnerabilities that might not be applicable to my environment or that I do not want to address, but there have been no false positives in my environment. In the last three years, I have only seen one vulnerability for which the patch was not released, but that was also a true positive. The only issue was that the OEM did not release the patch for that particular vulnerability.

“My final score for Qualys Enterprise TruRisk Management is eight out of ten..”

Pramod Borana

Senior Manager at a financial services firm with 10,001+ employees

[Read full review](#) 

“I have some understanding about PeerSpot, and I have visited the website. PeerSpot is similar to TrustRadius. It takes reviews from customers or end users who are using the tools and technologies in the market, and then provides a total review of that tool.

“My team works with the [Qualys TotalCloud](#) and True [Risk Management](#) products, and they generate reports. As for hands-on experience with Qualys technologies, I navigate through the Qualys portal, and I only use CSAM and Qualys VMDR. Apart from that, I do not perform many other tasks in Qualys. I receive reports from my teammates who work in vulnerability management. They prioritize the vulnerabilities they have detected according to the workstation and servers, then they decide what to remediate and what to patch based on the priority.

“When I became SOC Lead, I also got the responsibility of administrator.

Additionally, I have other responsibilities where I check on my teammates to ensure they are carrying out their tasks. I play a kind of team lead role. I receive reports from them about workstation vulnerabilities, server vulnerabilities, remediation and patching plans. I also check if the cloud agent is deployed in all the assets. My teammates deploy the scanner appliances and carry out the discovery scans and network scans. In my [SIEM](#) tool, I observe a log ingestion spike when the Qualys VMDR scanner appliance is running scans. This is also something I need to manage to tune it out when there are Qualys IPs and internal IPs assigned to the Qualys VMDR scanner appliance. These are some of the tasks I carry out day to day.

“Regarding the effectiveness of asset tagging in managing risk exposure, I haven't focused much in that area, but I see asset tagging as beneficial for us, similar to how we use tags in CrowdStrike. We have tags for all the different assets, which include site, cloud account, and department. It is easy for us to differentiate the assets based on those tags. Whenever we are creating groups and deploying policies or actions on those groups, we can use tags for separating them. That is the extent of my knowledge in this area for now.

“We haven't utilized Qualys VMDR's integration with threat intelligence feeds in our security architecture because we have our [SIEM](#) tool, which is centralized with integrated threat intelligence from CrowdStrike.

“I need to discuss the use of platform analytics in Qualys VMDR with my team to determine if they are using it. I can bring my Qualys SME into a discussion to provide feedback because he has been using Qualys for a very long time and has considerable expertise with the tool.

“What improvements would I suggest for this product? From what I have heard and seen, more clarity in group operations in query-building and resolving cloud agent download issues would be beneficial. For my experience, what were the initial challenges when using this product? The cloud level issues, especially during configuration profile downloads, stand out.

“I would rate this product an eight overall..”

Vaibhav Ghule

Soc Lead & Edr Administration at Persistent Systems

[Read full review](#) 

“I speak a little English.

“I have experience with Check Point solutions and Microsoft solutions.

“I have a little experience with the product portfolio of Check Point, as I have worked with this brand in a product manager commercial profile.

“I sold a project two years ago about Check Point Harmony [SASE](#) or [SASE](#) product.

“In the last twelve months with Check Point, I have experience with the firewalls and Harmony Email, but not with SASE.

“With the Maestro lines, I have experience, but not with Quantum Force, as I have worked with Maestro and Harmony Email.

“With CrowdStrike, I have a little experience, something about five months.

“I have worked with Qualys Enterprise TruRisk Management and VMDR.

“In the cybersecurity view, I understand what is being said.

“I cannot understand the TrueConfirm capability or tool.

“I am not familiar with the term TrueConfirm for threat enrichment capability.

“Qualys is a reliable tool.

“It is beneficial so far because the market today needs to protect all these factors that use AI for taking confidential information from the company.

“My profile is more commercial, but I know about the deployment of these tools being easy for companies to be prepared for this; however, a good assessment is necessary to review the architecture of the customer for a good chronogram and good time for the development of these tools.

“For this tool, we do not need cloud deployment because it requires some server and deployment from the endpoints of the company, so I do not have this technical knowledge.

“Qualys has a good price for the benefits of the development of this tool.

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

LuisPerez11

QA Manager at a consultancy with 51-200 employees

©2026 PeerSpot, All Rights Reserved

[Read full review](#) 

“Qualys Enterprise TruRisk Management shows material impacts on security. For example, if we scan a UPI server from Qualys Enterprise TruRisk Management agent, it will show that if we are not going to update that UPI server, that UPI hardware, or that application, going forward, it will be risky to us. Anyone, even a small hacker, can exploit your server, lose your data, collect your data, and misuse it in a black market. Every parameter, small to small and high to high, each and every parameter Qualys Enterprise TruRisk Management identifies and shows in an alert way, functioning as a monitoring tool also. It shows the severity. If we are not going to close this vulnerability, then what will happen. Severity is there also. There are severity five, four, three, two, and one. If the severity is five, it is most critical, and that vulnerability needs to be closed as soon as possible.

“In the current place where I work, they have their own infrastructure with multiple servers. We usually get a monthly report of vulnerabilities. The vulnerability count around monthly is approximately twenty thousand, thirty thousand, or more every month. We get a report from the Qualys Enterprise TruRisk Management department showing what the vulnerabilities are. We need to find out the most potential vulnerability. Qualys Enterprise TruRisk Management shows that the most important things are operating system related criticality, application related, and third-party application related vulnerabilities. It aggregates the most potential criticality in a severity. Severity means how critical this vulnerability is. There are numbers from one to five, with five being the most critical vulnerability. When we get a report, there is a column as a criticality tier. We usually filter it out with tier five, so all the vulnerabilities that are the most potential come up. For example, if I filter out with the five-tier, it usually shows around the most potential vulnerability count of one thousand or two thousand. This is not only for one server. We manage around eight hundred to nine hundred servers. We get a report every month for all servers' vulnerabilities, and it is approximately thirty thousand plus. It shows each and every potential critical vulnerability. We found two or three for each server. If we want to patch or deploy that vulnerability on each server, we need to take downtime. We have limitations to patch the servers each day. For example, in one day, we can patch fifty servers. If we want to patch five hundred servers, within ten days, we close that potential vulnerability by taking downtime as per the scheduled time. Mostly we take downtime at night for the deployment and patching those vulnerabilities.

“Once we complete our side patching, as per the Patch Tuesday schedule when Microsoft releases their patches and security patches every second Tuesday, we do patches and close the vulnerability with the remedies Qualys Enterprise TruRisk Management shows you. After patching, we take a report and share with the security team that we have closed this vulnerability and kindly scan the servers for rescanning. After patching, we take a reboot, and then after reboot, we rescan the system. We ensure everything is as per the expectation or not, and we verify if the vulnerability is closed or not. We rescan all the systems, and after rescan, it shows the previous vulnerabilities are closed in our scanned system.

“Confidence comes when we do practical validation. If due to some vulnerabilities or some bugs or some loopholes, attackers attack the servers and successfully collect the data, we do the root cause analysis to understand why the server got compromised or data got compromised. In that case, we learn that the particular server has not been patched since the last one month, two months, or three months. Due to that, till now, this kind of attack has not happened in our infrastructure because we make sure that every month patches should be deployed on that particular server within one month, thirty days. It prevents the situation in which if Microsoft releases one security patch with some enhancement in security, we deploy that. It is not that a particular patch has total one hundred percent security enhancement. Every patch has a loophole and security enhancement both things. If we patch the system and after then, attackers will try to find out the loophole in that particular patch. But once they find the loophole, before that, the second patch will be released by Microsoft, and the second patch will be deployed on that particular server by the patching team. This is how all things work. The attacker will not get enough time. That is why monthly patching is most necessary. We call it patching or vulnerability management.

“Monitoring tools such as [Zabbix](#) provide real-time or active monitoring. [Zabbix](#) alerts provide alerts in different colors and criticality. For example, if there is one system that uses one hundred percent CPU utilization or memory usage, or disk space issue, these kinds of real environment monitoring will show. If you search some websites on Google, sometimes that website takes a long time to be visible on your device. That happens due to latency, and latency happens due to high memory utilization or RAM utilization. It is the time travel between the sender and

receiver. When you send the request to the server, the server will give a response to you. The latency depends on read and write data. Zabbix is used for that. It enhances user experience, prevents downtime, and provides latest alerts. It monitors each and everything.

“My overall review rating for Qualys Enterprise TruRisk Management is eight out of ten..”

Roshan Ugale

Junior Associate at ESDS Software Solution Pvt Ltd.

[Read full review](#) 

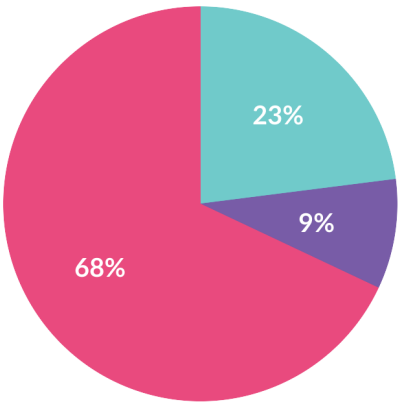
Top Industries

by visitors reading reviews

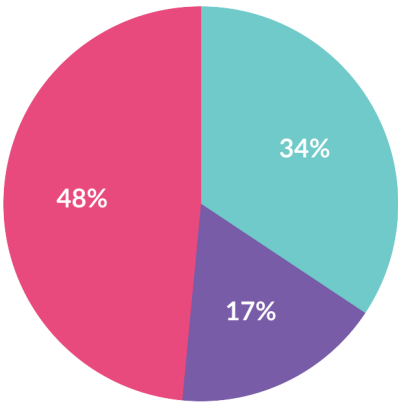


Company Size

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