aws marketplace

Qualys VMDR

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 9

Other Solutions Considered . . . . . 10 - 11

ROI . . . . . 12 - 14

Use Case . . . . . 15 - 16

Setup . . . . . 17 - 19

Customer Service and Support . . . . . 20 - 21

Other Advice . . . . . 22 - 24

Trends . . . . . 25 - 26

About PeerSpot . . . . . 27 - 28

Product Recap

Qualys VMDR

Qualys VMDR Recap

Vulnerability Management, Detection, and Response (VMDR) is a cornerstone product of the Qualys TruRisk Platform and a global leader in the enterprise-grade vulnerability management (VM) vendor space. With VMDR, enterprises are empowered with visibility and insight into cyber risk exposure - making it easy to prioritize vulnerabilities, assets, or groups of assets based on business risk. Security teams can take action to mitigate risk, helping the business measure their actual risk exposure over time.

Qualys VMDR offers an all-inclusive risk-based vulnerability management solution to prioritize vulnerabilities and assets based on risk and business criticality. VMDR seamlessly integrates with configuration management databases (CMDB), Qualys Patch Management, Custom Assessment and Remediation (CAR), Qualys TotalCloud and other Qualys and non-Qualys solutions to facilitate vulnerability detection and remediation across the entire enterprise.

With VMDR, users are empowered with actionable risk insights that translate vulnerabilities and exploits into optimized remediation actions based on business impact. Qualys customers can now aggregate and orchestrate data from the Qualys Threat Library, 25+ threat intelligence feeds, and third-party security and IT solutions, empowering organizations to measure, communicate, and eliminate risk across on-premises, hybrid, and cloud environments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Qualys VMDR provides a real-time response and reporting feature, which is excellent."

Ankesh Raj

Information Security Analyst at a tech services company with 51-200 employees

- "It allowed us to divide tasks easily among teammates, significantly improving efficiency."

Shubhajit Saha

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

- "The prioritization of vulnerabilities has improved our remediation efforts by around thirty to thirty-five percent."

Verified user

Works at a comms service provider with 1-10 employees

"It's also highly customizable, allowing us to tailor it to our needs."

Lakshay Grover

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

"It gives you a lot of options, and it integrates with our ServiceNow for ticketing and all."

MohitGupta2

Sr. Vice President Group Security at a financial services firm with 10,001+ employees

"Continuous monitoring is a crucial feature that we use more frequently."

Venkata Kalla

Information & security engineer at Infosys

"The most valuable feature is the vulnerability assessment."

VIKAS KUMAR YADAV

Solutions Architect at a consultancy with 10,001+ employees

What users had to say about valuable features:

"The most valuable feature is the QID part, especially of CentralList, which makes it easy to assess new critical vulnerabilities. It saves a lot in assessing and prioritizing risks to the organization.."

Saivarun Varun
IT Team Lead at a consultancy with 10,001+ employees

Read full review

"In Qualys VMDR, there are multiple valuable features such as Continuous Monitoring, SFU Connector, and WebVPN. Continuous monitoring is a crucial feature that we use more frequently.."

Venkata Kalla
Information & security engineer at Infosys

Read full review

"Qualys VMDR offers a one-stop solution for monitoring and reporting. The UI is straightforward and user-friendly, and even beginners can master it in a day.

It allows for simplicity in understanding issues and generating reports for clear visibility. The benefits of task division among teammates and the ability to work together without delays were significant.."

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

Read full review

"What I find valuable about Qualys VMDR is the capability of the tool and its user-friendliness. It is easy to use and provides accurate results, which is exactly what we are looking for. The prioritization of vulnerabilities has improved our remediation efforts by around thirty to thirty-five percent. The tool's integration between Patch Management and other Qualys products is also indispensable.."

Verified user

Works at a comms service provider with 1-10 employees

Read full review

"Qualys VMDR provides a real-time response and reporting feature, which is excellent. It allows us to see real-time graphs and reports for every asset, server, and more, which is very user-friendly.

Our clients have given good feedback, and they are satisfied with the tool. We use it daily to fix vulnerabilities by connecting with infrastructure to remediate. The feedback from the client side is very good.."

Ankesh Raj

Information Security Analyst at a tech services company with 51-200 employees

Read full review

“The most helpful and useful features of Qualys VMDR are its user-friendly design.

“Qualys VMDR is easy to understand and provides detailed reports.

“It impacts my workflow overall, with the patch management features as it has the missing patches listed in detail, making it easier to get a comprehensive report and providing some dashboards that offer visual representation..”

Nabanita Roy
JMS, RPSG Ventures Limited at RP Sanjiv Goenka Group

Read full review

Other Solutions Considered

"I have evaluated Rapid7 along with Qualys. In a rating out of five, I would give Qualys four and Rapid7 two, as Rapid7 is more complex and not as user-friendly.."

Ankesh Raj
Information Security Analyst at a tech services company with 51-200 employees

Read full review

"We worked with Nessus and Rapid7 before switching to Qualys VMDR. Qualys offers better pricing and more features compared to other tools. We did not find anything particularly missing from previous tools.."

Verified user
Works at a comms service provider with 1-10 employees

Read full review

"I have used another vendor for a different client, which is Rapid7. However, I found Rapid7 not as user-friendly as Qualys. The console is less user-friendly, and running sample templates or scans is more complex compared to Qualys.."

Ankesh Raj
Information Security Analyst at a tech services company with 51-200 employees

Read full review

"Before Qualys VMDR, we used Greenhorn's OpenVAS. It was open-source, but it offered no direct solutions. Reports were only available with scheduled scans, which made immediate issue resolution difficult.."

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

Read full review

"We also use Tenable Solutions for vulnerability management. However, Tenable requires manual processes for mitigation, whereas Qualys allows for automated mitigation of vulnerabilities and threats.."

Vikram Chakravarthy
T&S Specialist - Investigation and Prevention at Amazon

Read full review

"I did work on Tenable's POC and some other vendors. It has some limitations in detecting different types of vulnerabilities or false positives. Qualys is on the higher side when compared to the other tools.."

KiranReddy
Head of IT at a manufacturing company with 10,001+ employees

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
T&S Specialist - Investigation and Prevention at Amazon

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

Sr. Vice President Group Security at a financial services firm with 10,001+ employees

Read full review

Use Case

"We use it for vulnerability management and report generation mostly. I am trying to solve the issue wherein the stakeholders can get automated vulnerability reports to their mailbox.."

Verified user
Security Engineer at a consultancy with 10,001+ employees

Read full review

"We use Qualys VMDR for daily vulnerability management, scanning vulnerabilities, identifying vulnerabilities, reporting, creating dashboards, and the whole vulnerability management process. We also use it for patch management.."

Verified user
Works at a comms service provider with 1-10 employees

Read full review

"We use continuous monitoring to schedule scans for all the applications in our organization. We create a parent tag and sub-tags for each application and schedule scans based on our requirements, such as every alternate day, weekly, or monthly. This helps us identify vulnerabilities in the web applications, especially those that are public-facing.."

Venkata Kalla
Information & security engineer at Infosys

Read full review

"The primary use case for Qualys VMDR is for infrastructure vulnerability management. It assists devices, including all infrastructure devices like serverless network devices and development environments.."

Saivarun Varun
IT Team Lead at a consultancy with 10,001+ employees

Read full review

"We mostly use Qualys VMDR for vulnerability management and compliance practices. Every week, my team and I run automated scans that are scheduled, and we share whatever vulnerabilities are found with the infrastructure team to remediate them.."

Ankesh Raj
Information Security Analyst at a tech services company with 51-200 employees

Read full review

"The primary use case of Qualys VMDR was to monitor around two hundred users, servers, and VMs weekly. We needed to ensure that all vulnerabilities were tracked and addressed. Our users were mainly developers using various applications, and we needed to ensure compliance with client requirements. The goal was to keep our systems up-to-date and secure.."

Shubhajit Saha
System Admin at a tech services 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.

"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

Security Engineer at a consultancy with 10,001+ employees

Read full review

"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

Solutions Architect at a consultancy with 10,001+ employees

Read full review

"The initial setup of Qualys VMDR is straightforward. The setup's complexity depends on the organization's size and collaboration with various teams. For organizations with a clear device inventory, the deployment can be completed within a month.."

PratikDesai

Senior Global IT Security Specialist at a manufacturing company with 1,001-5,000 employees

Read full review

"The initial setup is agent-based and straightforward, especially if you have necessary tools like Active Directory. Given the cloud-based nature of Qualys, deployment can be completed within a day with appropriate resources.."

Vikram Chakravarthy

T&S Specialist - Investigation and Prevention at Amazon

Read full review

“It's not an issue with Qualys itself. We encountered some problems when migrating from physical scanners to virtual ones, but that was more on our network team’s side. Qualys provided excellent support in that scenario, which helped us identify and resolve the issue on time, and we provided the solution to our customer.

I work with the on-premises version. We updated from physical scanners to virtual scanners.

In my previous organization, I worked on deploying the solution. There, I customized the Windows OS image so that when you install the image on any machine, it prompts for a key that’s already embedded. Once the steps are completed, it automatically installs the Cloud Agent module on every machine. The agent syncs data every four hours, providing vulnerability data and security insights for each machine.

It’s not a one-person task. We had to coordinate with several teams, such as the network and system teams, for deployment. In total, we worked with about six teams during the process.

For about 1,400 machines, it took around three months to complete the deployment and resolve any issues. For example, sometimes policies weren't pushed properly from Ivanti or other tools, or users didn’t turn on their machines, which stopped Qualys services. We had to address these issues for each user, so it took some time. But we completed the deployment in about three months.

Maintenance isn't difficult, especially when working with the Cloud Agent. You just need to set up rules, like purging machines that haven’t connected to the network in three months. You write policies to manage this, which simplifies the decommissioning process and other tasks..”

Lakshay Grover

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

Read full review

Customer Service and Support

"When you raise a report, it will be generated in VMDR and shared with the respective team. Depending on client requests, reports can be in PDF or Excel format.."

Verified user
System Engineer at a financial services firm with 1-10 employees

Read full review

"I have heard that their technical support team is very responsive and takes quick action when needed. However, I have never interacted with them personally.."

VIKAS KUMAR YADAV
Solutions Architect at a consultancy with 10,001+ employees

Read full review

"The customer support system could be improved. While they respond, it takes them two to three days to address a concern, which is an issue. Overall, I would rate customer service as five or six.."

Venkata Kalla
Information & security engineer at Infosys

Read full review

"We have a dedicated person for support. She's always available to help, or if she's on leave, she ensures someone else is aligned to handle our cases, so we don't breach any timelines. I'd give the support a high rating.."

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

Read full review

"I am satisfied with the support of Qualys VMDR as they are supportive. However, there are sometimes issues where we cannot talk to customer support directly, and we have to raise tickets, which sometimes takes a lot of time to resolve issues because it goes through their own phase. We cannot change the SLA or the priority of the tickets, so that is an issue.."

Nabanita Roy
JMS, RPSG Ventures Limited at RP Sanjiv Goenka Group

Read full review

"The technical support is slow to respond. Most likely, they just provide reference links for documentation instead of offering in-depth technical guidance. This level of support doesn't compare well to others like Cisco, Juniper, or Avaya, which offer more hands-on assistance.."

Verified user
Senior Application Security Engineer at a real estate/law firm with 501-1,000 employees

Read full review

Other Advice

"I would recommend getting both VMDR and the Cloud Agent to ensure comprehensive asset coverage. Understanding the network architecture is crucial to ensure no segments are missed under Qualys. Overall, I rate Qualys a nine out of ten.."

Verified user
Works at a comms service provider with 1-10 employees

Read full review

"I would recommend Qualys VMDR to the other stakeholders because it already has its place in the market, and it's very reliable.

I'd rate the solution eight out of ten.."

Verified user
Security Engineer at a consultancy with 10,001+ employees

Read full review

"I recommend Qualys VMDR as it effectively reduces the time required for vulnerability management and operates well with fewer people.

I'd rate the solution seven out of ten.."

Venkata Kalla
Information & security engineer at Infosys

Read full review

"Users should go through the training offered by Qualys for all VMDR modules and take an introductory call on how to use and schedule tasks. Setting up one thing at a time and testing the desired results before moving on is advised.

I'd rate the solution eight out of ten.."

Nabhanyu Halgeri
Cyber Security Specialist at a tech services company with 51-200 employees

Read full review

"I would recommend Qualys VMDR to others comparing it with other VM tools, due to its valuable features, including real-time responses and detailed reporting.

Overall, I would rate Qualys eight out of ten. With potential improvements and AI integration, it could offer even more.."

Ankesh Raj
Information Security Analyst at a tech services company with 51-200 employees

Read full review

"I would recommend Qualys VMDR because it ensures comprehensive coverage, including aspects like vulnerability management and PCI, providing good inputs and improvements over time.

I'd rate the solution nine out of ten.."

Saivarun Varun
IT Team Lead at a consultancy with 10,001+ employees

Read full review

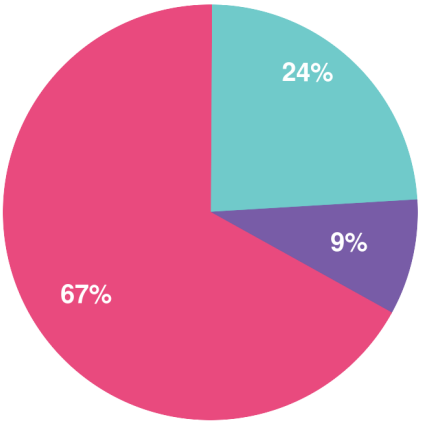
Top Industries

by visitors reading reviews

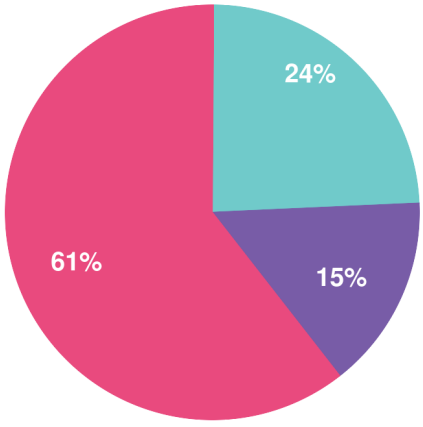
Financial Services Firm	16%
Computer Software Company	12%
Manufacturing Company	8%
Government	7%

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 software running on AWS and other platforms. 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