aws marketplace

Tenable Vulnerability Management

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Tenable Vulnerability Management

Tenable Vulnerability Management Recap

Tenable Vulnerability Management offers efficient scanning, reporting, and integration capabilities. It supports extensive visibility and risk management for diverse environments while providing a user-friendly experience with strong cloud capabilities and container scanning.

Tenable Vulnerability Management is crucial for vulnerability assessment and managing security across network infrastructures. It effectively handles cloud and on-premises scans, identifying risks and enhancing cybersecurity measures with detailed reports. With features like automated scanning and risk prioritization, users manage vulnerabilities efficiently. Despite its strong points, improvements in pricing, navigation, and customization are desired, alongside better integration and AI-driven detection.

What are the most important features of Tenable Vulnerability Management?

- Automated Scanning: Simplifies the identification of vulnerabilities through efficient scans.
- Comprehensive Reporting: Offers detailed insights into potential security risks.
- Seamless Integration: Easily connects with third-party tools for extended functionality.
- Cloud Capabilities: Provides strong security management in cloud environments.
- Container Scanning: Specialized in scanning containerized applications for threats.
- Real-time Prioritization: Helps prioritize vulnerabilities for effective resolution.

What benefits and ROI should users look for?

- Enhanced Security Posture: Achieves improved overall protection from threats.
- Efficient Risk Management: Streamlines the process of identifying and mitigating risks.
- Extensive Visibility: Offers a clear understanding of assets and vulnerabilities across the network.
- Scalability: Adapts to varying organizational sizes and needs effectively.

In industries like finance, healthcare, and education, Tenable Vulnerability Management supports robust cybersecurity measures. Organizations utilize it for scanning IT infrastructures, conducting cloud assessments, and performing endpoint analysis to mitigate threats in critical environments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Tenable Vulnerability Management agents are very lightweight, and the results we get are very accurate."

Chethan Gowda

Windows Security Patching Operation III (Cyber Operations) at CBTS

- "The ease of use, the automated scanning facility, and their good support mechanism are all valuable."

TarunKumar2

Deputy Global Chief Information Security Officer at Nissan Digital

- "Tenable is user-friendly and excels in reporting."

Mani Bommisetty

Infrastructure patching Manager at a manufacturing company with 1,001-5,000 employees

"The main benefits that Tenable Vulnerability Management provides for me as an end user include saving time and money and streamlining processes."

Arnab-Paul

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

"Tenable Vulnerability Management is the backbone of our vulnerability management and has affected my organization positively."

Verified user

SOC Analyst at a energy/utilities company with 1,001-5,000 employees

"The stability is commendable, and I would rate Tenable ten out of ten."

Rishabh-Khanna

Technical Lead at a healthcare company with 10,001+ employees

"The integration of Tenable into our security ecosystem was very good."

HARI EDARA

IT Manager at State of Texas

What users had to say about valuable features:

"Currently, I have only used Tenable for DOS attack-related purposes and thus, I am not fully acquainted with its other features. However, it provides survivability benefits. It helps me understand if the system is capable of withstanding certain levels of stress. Though it's not core technical security testing, it provides us with survivability insights.."

Rishabh-Khanna
Technical Lead at a healthcare company with 10,001+ employees

Read full review

"Tenable is user-friendly and excels in reporting. It allows me to easily fetch and schedule reports. The software's discovery feature aids in strengthening our security posture. The single-sensor installation process on various operating systems is smooth, unlike Rapid7, which requires different versions for separate systems. Furthermore, Tenable enables vulnerability management through potential AI integration that consolidates efforts and resolves multiple vulnerabilities simultaneously.."

Mani Bommisetty
Infrastructure patching Manager at a manufacturing company with 1,001-5,000 employees

Read full review

"The functions and features of the product that I find most useful in Tenable Vulnerability Management are noteworthy. I am satisfied with the analytics and reporting part of Tenable Vulnerability Management. Real-time risk prioritization in Tenable Vulnerability Management is useful for my security strategy. The main benefits that Tenable Vulnerability Management provides for me as an end user include saving time and money and streamlining processes.."

Arnab-Paul
Cyber Security Consultant at a tech vendor with 10,001+ employees

Read full review

"I think their automated vulnerability scan and the scanning engine of Tenable Vulnerability Management are valuable. There are agents that you can deploy, and you can run the scans on those IPs on an automated basis. The automated scanning feature is probably the most important. They also have a good remediation workflow which can be integrated with your own internal workflow. You can do automated tracking of closure of the vulnerabilities. The ease of use, the automated scanning facility, and their good support mechanism are all valuable. If you were to get stuck somewhere, they can readily make their customer service or technical teams available to take care of our needs. Automated vulnerability scanning is the feature which makes life a little easier.."

TarunKumar2
Deputy Global Chief Information Security Officer at Nissan Digital

Read full review

Tenable Vulnerability Management agents are very lightweight, and the results we get are very accurate. The solutions they provide to us, assuming if one vulnerability exists, there will be a solution. The resolution they give us in wording will be the best solution. The exploit rates and the reports we get provide a lot of information, making it very easy for us to verify.

The main benefit of integration with Tenable Vulnerability Management is that there will be no lack of missing vulnerabilities when it comes to the patching environment. That is one of the key aspects of why we have integrated Tenable to our patching tools. It has a vast capacity of pushing the data to our tools due to its capability and compatibility. That is also one of the reasons why we are using Tenable Vulnerability Management. ."

Chethan Gowda
Windows Security Patching Operation III (Cyber Operations) at CBTS

Read full review

"The best features of Tenable Vulnerability Management are flexibility, breadth and scope, and the fact that their current vulnerabilities come out, and they have tests for them within a day or two.

"Operationally, Tenable Vulnerability Management finds issues that would otherwise be missed, but I don't have an ROI.

"The impact of Tenable's analytic capabilities shows that our other programs are working in our prioritization process.."

Verified user
SOC Analyst at a energy/utilities company with 1,001-5,000 employees

Read full review

Other Solutions Considered

Before Tenable Vulnerability Management, we used Qualys initially. We moved to Tenable due to pricing considerations. The customer requirement was to reduce the cost. When compared to Qualys, it was much more cost-effective.

Chethan Gowda
Windows Security Patching Operation III (Cyber Operations) at CBTS

Read full review

We have not validated other options before choosing Tenable Vulnerability Management. We have already worked with multiple tools, and the customer was very interested in Tenable Vulnerability Management specifically.

Chethan Gowda
Windows Security Patching Operation III (Cyber Operations) at CBTS

Read full review

“I used Rapid7, which is less expensive than Tenable. My preference now aligns with Tenable due to its superior user-friendliness and reporting capabilities, although some issues persist with installation complexity in various environments..”

Mani Bommisetty
Infrastructure patching Manager at a manufacturing company with 1,001-5,000 employees

Read full review

"I don't know why we switched to Tenable Vulnerability Management for vulnerability management, but my assumption is that it is the first solution they tried and we've been happy with it since.."

Verified user
SOC Analyst at a energy/utilities company with 1,001-5,000 employees

Read full review

"I would recommend HP WebInspect, having used it for around two and a half years. It offers both cloud and standalone versions, both of which are fantastic. It is applicable for both legacy applications and the latest applications in the market. HP WebInspect features extensive libraries and recursive methods to traverse everything, which I find really impressive.."

Rishabh-Khanna
Technical Lead at a healthcare company with 10,001+ employees

Read full review

"We have used QualysGuard before using Tenable Vulnerability Management.

"We decided to switch from QualysGuard to something else because these were two different companies. This was the previous company where I had exposure to QualysGuard. We have never made any change from Tenable in the current company.."

TarunKumar2
Deputy Global Chief Information Security Officer at Nissan Digital

Read full review

ROI

Real user quotes about their ROI:

"The product impacts our client's operational cost related to vulnerability management in a good way. It automates a few things and saves the engineers' costs.."

Sirish Kumar
Director at Inspyretek Solutions

Read full review

"We see a return by identifying vulnerabilities and converting them into actionable items. The solution provides a lot of visibility into your environment. ."

Yusuf-Hashmi
Sr. Director - Group Head - IT Security (CISO) at Jubilant Organosys Ltd., India, Leading Chemical M

Read full review

"I saw a return on investment from using the solution since I feel that finding the vulnerabilities is always much cheaper than dealing with a situation after your system gets hacked. In short, I would put it as insurance is cheaper than the fire.."

Verified user
IT Manager at a financial services firm with 1,001-5,000 employees

Read full review

For evaluating the effectiveness of Tenable Vulnerability Management in our IT environment, we have our own ratings with integrated multiple metrics that automatically calculate. It has been integrated into our ServiceNow. Based on that, all the overall metrics are automatically calculated based on AI and ML technology, where we get complete reports.

Chethan Gowda
Windows Security Patching Operation III (Cyber Operations) at CBTS

Read full review

“I have experienced a return on investment using Tenable.io. It showed us what we did wrong in the process of building the vulnerability management program in our company. It also gave us an understanding, making it a good solution.

On a scale of one to ten, where one is no return on investment, and ten is a hundred percent return on investment, I rate the solution a seven.

.”

Shay Chouker
CSO at Altera

Read full review

Use Case

"We use the Tenable Vulnerability Management solution for internal web applications, asset management, and remediation. It helps us transfer and leverage the remediation of websites, effectively addressing vulnerabilities.."

Kelvin Oladipo
Team Lead, Cyber Security at Uridium Technologies

Read full review

"We don't have a specific use case. My primary purpose for using Tenable is to conduct survivability tests, mainly to determine whether the system crashes, particularly when subjected to DOS attacks. I do not use it for more than that because, for other aspects, we have manual VAPT procedures in place.."

Rishabh-Khanna
Technical Lead at a healthcare company with 10,001+ employees

Read full review

"I use Tenable Vulnerability Management to scan the network, including servers and endpoints, to identify risks in our environment and provide mitigation and solutions. I also use it to assess our security posture through asset discovery and risk identification.."

Mani Bommisetty
Infrastructure patching Manager at a manufacturing company with 1,001-5,000 employees

Read full review

"My experience is with Tenable Vulnerability Management, specifically regarding vulnerability management.

"My particular use case for Tenable Vulnerability Management is vulnerability management, benchmark scanning, and I'm somewhat familiar with their product line, utilizing the CIS benchmarks and DISA STIG benchmarks.

"Tenable Vulnerability Management is the backbone of our vulnerability management and has affected my organization positively.."

Verified user
SOC Analyst at a energy/utilities company with 1,001-5,000 employees

Read full review

"I think we use Tenable Vulnerability Management primarily for our internal use. We are not a reseller; we are a customer.

"We have a set of IPs across the globe, and we conduct this scan once a quarter of all the IPs combined. This scanner has updated information with respect to vulnerabilities that exist in the open. We perform vulnerability scans of all the IPs in order to ensure that no vulnerability exists in our environment, infrastructure, or network. We run vulnerability scans which are automated in nature and scheduled over the weekend to make sure that all the IPs are up to date. Once in a quarter, all IPs are scanned and a vulnerability report is generated. This report tells us whether there are low, medium, or high critical vulnerabilities that exist. We have a remediation plan for the high, medium, and low vulnerabilities in terms of the amount of time that we should be taking in order to patch these vulnerabilities. This tool keeps our information security posture high. We also carry out aging analysis because there are some vulnerabilities that cannot be patched due to dependencies. We actively carry out aging analysis in order to see if there are some vulnerabilities that are still in the system for more than one month or two months, and what the reason is. We actively work with all of the business teams and the IT setup within our system is quite regimented in order to run the scans once in a quarter for all the IPs.."

TarunKumar2
Deputy Global Chief Information Security Officer at Nissan Digital

Read full review

We usually use Tenable Vulnerability Management for vulnerability scannings, and we get the reports from Tenable to resolve any vulnerability. We have about 2,000 plus servers where we have installed the agent on those servers to check and scan the vulnerabilities. That is the main key aspect of what we use Tenable Vulnerability Management for.

Regarding the continuous monitoring feature of Tenable Vulnerability Management, it is not exactly continuous monitoring we get from Tenable. It is used only on the market, where we scan it. We have a scheduled scan for all the servers, so we are not using it for any monitoring at present.

“Tenable's advanced analytics and reporting features give very detailed reports where we get most of the information about vulnerabilities. That is one plus point. For example, with 2,000 servers, when we want to calculate the percentage of vulnerabilities that have appeared, it gives us very useful insights. While analyzing, it is one of the greatest tools because the results it produces as outputs scan the networks and each device in an organization.

“We have purchased Tenable Vulnerability Management via AWS Marketplace. .”

Chethan Gowda
Windows Security Patching Operation III (Cyber Operations) at CBTS

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 not straightforward. We need to apply the filters. We can get the Cyber Exposure Score displayed on the document. However, we cannot get a deeper understanding of what makes the score high or low.."

HARI EDARA

IT Manager at State of Texas

Read full review

"The configuration is easy. My engineers can work on it seamlessly. The deployment of the basic solution does not take more than four to eight hours. We need one or two persons to deploy and maintain the product. There are no other challenges if we have the network and can access the IPs.."

Sirish Kumar

Director at Inspyretek Solutions

Read full review

“The product's initial setup was very straightforward.

The solution is deployed on an on-premises model and the cloud. With the endpoint in the product, everything was reported back to the cloud offered by Tenable..”

Verified user

Read full review

IT Manager at a financial services firm with 1,001-5,000 employees

“The tool's deployment can be challenging, especially for those unfamiliar with Kali Linux, as it operates on this platform. This might make the setup process difficult for users accustomed to other operating systems like Windows. It may take a couple of tries to get comfortable with the process. However, once you have set it up a few times, it becomes easier..”

DivyaJyoti

Read full review

0

"The product is complicated to set up on AWS. However, it is easy to implement on-premises. It involves discovering IP addresses and schedule scanning. It requires acquiring some knowledge about the process to familiarize yourself with the AWS environment. We have to complete the setup for the whole environment. The deployment for a vast environment involves migrating a lot of data from on-premise to the cloud.."

Donald Koketso

Read full review

Security engineer at a construction company with 1,001-5,000 employees

"I would rate my experience with the initial setup a nine out of ten, with ten being very easy to set up.

We offer both deployment models, cloud as well as on-premises, but the cloud model hasn't been very successful. Because Cloud deployment is a SaaS model, which will likely be expensive.

There are cost concerns with SaaS.

Deployment is quick.

The entire deployment took around one hour.."

Yogeswaran Neelagandan

Read full review

Key Account Manager at Uniware

Customer Service and Support

"The solution's support is okay, but it could be more customer-friendly. The people providing support have knowledge, but they could improve customer interaction.."

DivyaJyoti
0

Read full review

"Technical support from Tenable is rated six out of ten. It needs improvement in response time and addressing feature requests promptly. Other services like Rapid7 are more responsive.."

Mani Bommisetty
Infrastructure patching Manager at a manufacturing company with 1,001-5,000 employees

Read full review

"Customer support is a challenge. Tenable charges extra for it, which means clients have to buy the license separately and then pay for additional support services like SQ. This creates significant friction. ."

Yogeswaran Neelagandan
Key Account Manager at Uniware

Read full review

"We had used Tenable's expert support services in order to make sure that we run Tenable Vulnerability Management on a continuous basis and are able to utilize their services. At the time of the implementation, we had taken the help of Tenable's expert support to be able to help us use this feature at the outset.."

TarunKumar2
Deputy Global Chief Information Security Officer at Nissan Digital

Read full review

"I would evaluate Tenable Vulnerability Management's customer service and technical support as average.

"I would rate them a seven on a scale from 1 to 10, with 10 being the best and 1 the worst.."

Verified user
SOC Analyst at a energy/utilities company with 1,001-5,000 employees

Read full review

Communication with Tenable Vulnerability Management support occurs on average two to three times monthly because our environment is very small.

The technical support of Tenable Vulnerability Management is available 24/7, and whenever we require support, we can get it within five minutes. Regarding technicality, they deserve a nine out of ten. They are highly technical people. I have communicated with more than 20 to 25 technical engineers. They take every question seriously and help us resolve issues. They have a very strong technical team to support customers. .”

Chethan Gowda
Windows Security Patching Operation III (Cyber Operations) at CBTS

Read full review

Other Advice

"I have purchased a license directly from Tenable, so I am working directly with Tenable and not through partners. My overall review rating for Tenable Vulnerability Management is eight.."

Arnab-Paul
Cyber Security Consultant at a tech vendor with 10,001+ employees

Read full review

"I recommend Tenable Vulnerability Management for its comprehensive security capabilities and effective risk identification. However, potential users should be prepared for the higher expense compared to alternatives like Rapid7.

My rating is eight out of ten, mainly due to the support aspect needing improvement.."

Mani Bommisetty
Infrastructure patching Manager at a manufacturing company with 1,001-5,000 employees

Read full review

We use Tenable Vulnerability Management and are currently using its latest version.

I rate Tenable Vulnerability Management nine out of ten based on my experience. This rating is due to its stability and high scalability. The best part is the solutions they provide for any vulnerability. ."

Chethan Gowda
Windows Security Patching Operation III (Cyber Operations) at CBTS

Read full review

"I would rate it four out of ten. For startups, freelancers, or companies between startup and midsize, Tenable is recommended. However, for midsize or enterprise-level companies, I would not prefer it. We use it because the client suggested it. Otherwise, my preferences might differ. The type of application matters, too. For new applications, such as those based on Node.js, Tenable could be a good option. However, for legacy technologies with complex databases, newer systems like Tenable are not recommended. If the budget allows, HP WebInspect is preferable. Budget considerations are as important as choosing the right technology. If limited by budget, Tenable is a viable option for new, growing companies, but not for enterprises. Overall, I rate the solution four out of ten.."

Rishabh-Khanna
Technical Lead at a healthcare company with 10,001+ employees

Read full review

"I have used Tenable Vulnerability Management's reporting features to a lesser degree.

"The metrics I track for decision-making include what systems need upgrading, what software needs replacing, and whether or not we can hold off on things,

accept some risks, and get other risks resolved.

“They have cloud scanners that are effectively point and click, and although I'm not sure if it's an extra licensing, we also have an on-prem scanner, which is a virtual appliance that I can download and put in place.

“The data that we pull from Tenable Vulnerability Management is the data that we drive and use for decision-making, although we don't use that visibility extensively. I don't utilize the real-time visibility with Tenable Vulnerability Management.

“On a scale of 1-10, I rate Tenable Vulnerability Management a 9..”

Verified user
SOC Analyst at a energy/utilities company with 1,001-5,000 employees

Read full review

“I use Tenable Vulnerability Management, and that is the tool that I have primary experience with.

“Apart from zero-day vulnerability, which obviously none of the tools would know about, I think the scanning engine of Nessus, part of Tenable Vulnerability Management, is quite up-to-date. It provides details on how the remediation should take place and provides detailed steps on how the remediation can be undertaken, which is quite helpful for the various application teams in order to understand. Their platform is something which is quite up-to-date. It appears that in the back-end they have the right set of threat intelligence feeds that come in from all different sources. I would assume that their AI engine and also their database is quite updated. From the perspective of being up to date, we feel very comfortable because we do rely on and trust their AI engine which their scanning facility is powered with.

“The importance of real-time risk prioritization for our organization's security strategy is very high. These are the times where you cannot really go loose at all.

Remediation becomes prioritized for all organizations. It is extremely important that at least the highly critical vulnerabilities are patched within 24 to 48 hours because they are high targets and valuable targets for adversaries. Therefore, risk prioritization is probably extremely important for organizations to keep these in the highest priority of any activity.

“We have not yet integrated Tenable Vulnerability Management as much. We are using Tenable on a standalone basis. We have not yet done an integration with any GRC tool or any other tool. As of now, we are using Tenable as an independent tool.

“Tenable Vulnerability Management is deployed on-cloud in our organization, and we are using Amazon Web Services as our cloud provider.

“I would give Tenable Vulnerability Management a nine out of ten rating. This is not a matter of concern because, apart from the costing part, which was pretty much okay when we signed up, over a period of time they have been increasing their license fee. That is the only point which I believe that they could possibly look at working upon. Otherwise, it is a nine out of ten for sure. My overall review rating for Tenable Vulnerability Management is eight out of ten..”

TarunKumar2
Deputy Global Chief Information Security Officer at Nissan Digital

Read full review

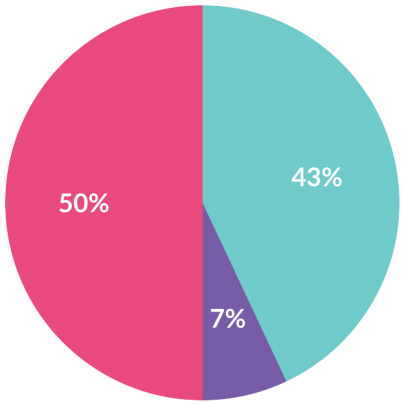
Top Industries

by visitors reading reviews

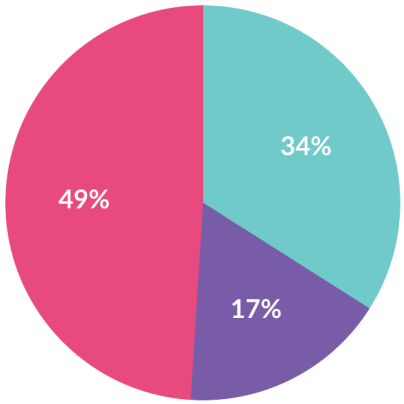
Financial Services Firm	14%
Manufacturing Company	9%
Outsourcing Company	7%
Computer Software Company	7%

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 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