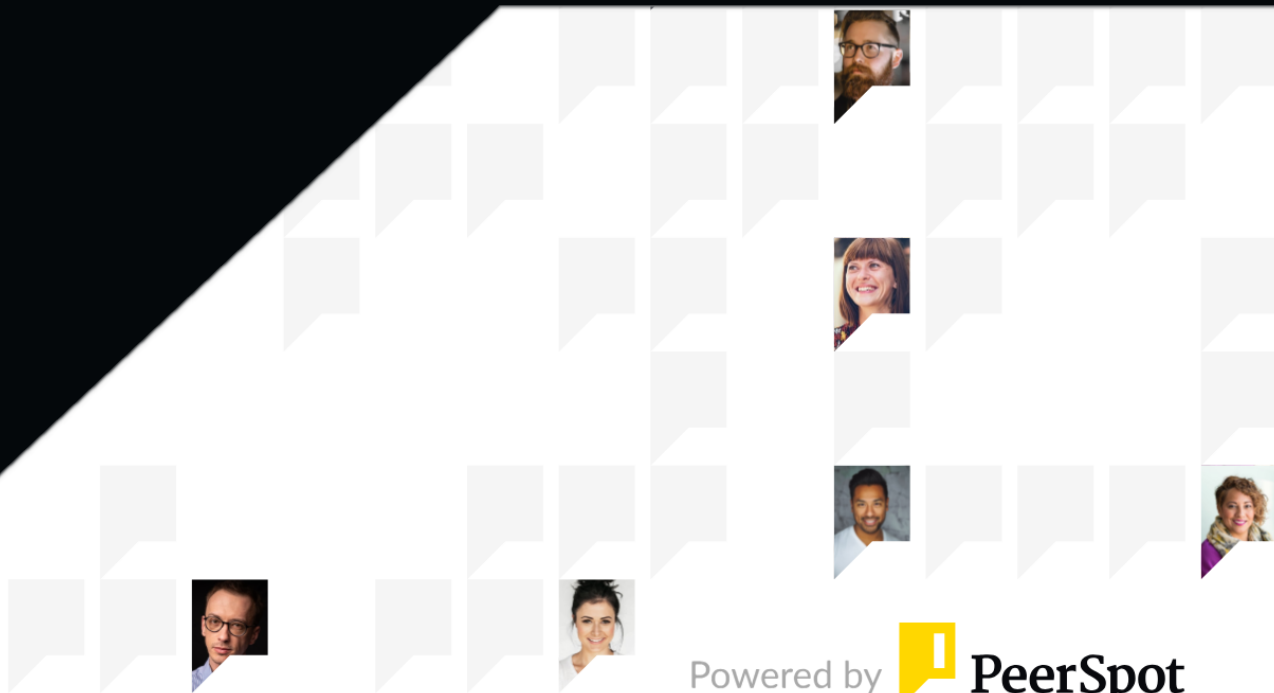


aws marketplace

Tenable Cloud Security

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 10

Other Solutions Considered..... 11

Use Case..... 12 - 15

Setup..... 16 - 17

Customer Service and Support..... 18 - 19

Other Advice..... 20 - 23

Trends..... 24 - 25

About PeerSpot..... 26 - 27

Product Recap



Tenable Cloud Security

Tenable Cloud Security Recap

Tenable Cloud Security is a comprehensive solution designed to help organizations secure their cloud environments across various platforms, including AWS, Azure, and Google Cloud. It offers continuous visibility, compliance management, and threat detection to ensure that cloud infrastructure and applications are protected from vulnerabilities and misconfigurations.

Tenable Cloud Security exemplifies a comprehensive Cloud-Native Application Protection Platform (CNAPP) by providing a unified solution that covers the entire cloud security lifecycle, from development to runtime. This platform is designed to address vulnerabilities, misconfigurations, threats, and compliance risks across multi-cloud environments, making it an essential tool for organizations adopting cloud-native architectures. In practice, Tenable Cloud Security integrates security into the development process through its shift-left approach, particularly with Infrastructure as Code (IaC) security. This ensures that security measures are embedded early in the development lifecycle, allowing teams to identify and mitigate vulnerabilities before they reach production. Once in production, the platform continues to provide real-time visibility into cloud environments, enabling continuous monitoring and proactive threat detection.

The solution's comprehensive protection spans various aspects of cloud security, including the identification and remediation of misconfigurations, automated compliance management, and advanced threat intelligence. By automating these processes, Tenable Cloud Security reduces the manual effort required to manage cloud security, freeing up resources for more strategic initiatives.

What are the key features of Tenable Cloud Security?

- **Unified Platform:** Covers the entire cloud security lifecycle, from development to runtime, providing comprehensive protection.
- **Shift-Left Approach with IaC Security:** Integrates security early in the development process, ensuring that vulnerabilities are caught and remediated before deployment.
- **Continuous Monitoring:** Offers real-time visibility and monitoring of cloud environments, enabling proactive threat detection and response.
- **Automation:** Streamlines security operations, reducing the need for manual intervention and increasing operational efficiency.
- **Comprehensive Threat and Compliance Management:** Identifies and mitigates vulnerabilities, misconfigurations, and compliance risks across multi-cloud environments.

What are the benefits of using Tenable Cloud Security?

- **Improved Security Posture:** Early detection and remediation of vulnerabilities lead to a stronger overall security posture.

- **Operational Efficiency:** Automation reduces the workload on security teams, allowing them to focus on higher-priority tasks.
- **Risk Reduction:** Proactively identifies and addresses risks before they impact production environments.
- **Simplified Compliance:** Helps organizations meet and maintain compliance with industry standards, reducing the complexity and cost of audits.

Tenable Cloud Security is particularly valuable in industries with stringent regulatory requirements, such as finance, healthcare, and retail. For example, in the financial sector, it helps organizations ensure compliance with regulations like PCI-DSS while safeguarding sensitive data across cloud environments.

In summary, Tenable Cloud Security is a robust CNAPP solution that integrates security throughout the cloud lifecycle, providing comprehensive protection and operational efficiency for cloud-native environments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Element is precisely what we needed for close to real-time external surface monitoring, and the automatic integration capabilities, particularly with DNS, Azure, and AWS, are extremely valuable.”



DragosCernat

Information Security Architect at WSP

- ✓ “The analytical and reporting capabilities are pretty straightforward and show every transaction and major attempt to attack the application in the cloud.”



Antonio Scola

Owner at SUNLIT TECHNOLOGIES

- ✓ “Scanning and reporting are the most valuable features of Tenable Cloud Security”



Javeed Abdul

Senior System Engineer at a tech consulting company with 10,001+ employees



“The solution’s vulnerability management feature has helped us identify and mitigate risks well.”



HARI EDARA

IT Manager at State of Texas



“The tool alerts us on depreciating performance or deficiencies of our web application. It helps us react on time.”



Rob Hussey

System Administrator at OnShift



“Tenable Cloud Security has positively impacted my organization with risk reduction and compliance.”



Andrew Lane

Cloud Security Engineer at a tech vendor with 51-200 employees



“The product's deployment phase is easy.”



Trirong Phuaythip

Solution Consultant at Westcon-Comstor

What users had to say about valuable features:

“Tenable Cloud Security is used for CSPM. If you have multi-cloud tenancy using AWS and Azure, you can have a single dashboard where you can onboard all the cloud infrastructure and have visibility into it. It has multiple cover steps of compliance. So, if you are obliged by any compliance, you can use that particular compliance..”

SumeshKumar

Manager Cloud Security at Hitachi Systems, Ltd.

[Read full review](#) 

“From what I know, though I'm not an expert technically speaking, perhaps the best functionalities are related to promoting a deeper analysis of the environment where applications are running in terms of creating a double armor of security to block threats that may come in the cloud with Tenable Cloud Security.

Companies are looking for cloud security, specifically Tenable Cloud Security, because they know it's a reliable company with long-term presence in the market, and they trust Tenable for their product strategy and support. This is the main reason. .”

Antonio Scola

Owner at SUNLIT TECHNOLOGIES

[Read full review](#) 

“The best features Tenable Cloud Security offers in my experience are automatic scanning, frequent scanning, and automatic finding, which I find valuable.

“Tenable Cloud Security has positively impacted my organization with risk reduction and compliance.

“We weren't previously measuring compliance, so that's completely new to our organization regarding risk reduction and compliance improvements..”

Andrew Lane

Cloud Security Engineer at a tech vendor with 51-200 employees

[Read full review](#) 

“Tenable Cloud Security excels in vulnerability detection, one of its strongest features. Another valuable feature is software composition analysis, which highlights and automates the detection of security flaws. Additionally, their knowledge base is excellent; if anything goes wrong, they provide clear guidance on what needs to be done to address specific vulnerabilities.

The asset management is also really good, with effective discovery and categorization of assets. The DevOps integration is also strong, supporting Shift-Left Security practices with integration into pipeline tools..”

Ondrej Kováč

Solution Engineer at Exclusive Networks Czechia

[Read full review](#) 

“The solution is good. We integrated our AWS account with Tenable Cloud Security for security and compliance. The IAM features are valuable. We can analyze the permissions of the users in all the aspects of AWS. The solution’s vulnerability management feature has helped us identify and mitigate risks well. I can do the scans from the on-premise and cloud solutions. The tool integrates well with our existing products. We have integrated it with ServiceNow. It works well..”

HARI EDARA

IT Manager at State of Texas

[Read full review](#) 

“Element is precisely what we needed for close to real-time external surface monitoring. The automatic integration capabilities, particularly with DNS, Azure, and AWS, are extremely valuable. The platform automatically collects records and adds assets, eliminating the need for daily manual checking and updating.

“The streamlined process ensures that all new assets are automatically added to the platform, reducing manual labor and making the system more proactive. The ease of communication with the Element team and their responsiveness to integration needs has been particularly beneficial..”

DragosCernat

Information Security Architect at WSP

[Read full review](#) 

Other Solutions Considered

“Products like Fortinet, Qualys, and Rapid7 offer the same set of services. The only common issue I found between all the products was that though the tools can be deployed on the cloud services offered by Microsoft, AWS, and Google, the products cannot be deployed on Oracle.

I am in the process of testing different solutions from vendors like Rapid7 and Qualys..”

Verified user

Solutions and Services Manager at a tech services company with 11-50 employees

[Read full review](#) 

Use Case

“The most popular use cases include vulnerability detection, cloud security posture management, software composition analysis (comparing code), and supporting cloud-native application protection in runtime environments..”

Ondrej Kováč

Solution Engineer at Exclusive Networks Czechia

[Read full review](#) 

“They are looking to promote a deeper security strategy with Tenable Cloud Security. Companies are migrating from on-premise to clouds and they must ensure their applications in the cloud will be more safe and secure.

Healthcare is most likely the kind of clients we see migrating to Tenable Cloud Security. .”

Antonio Scola

Owner at SUNLIT TECHNOLOGIES

[Read full review](#) 

“Tenable Cloud Security is used for scanning purposes, including vulnerabilities and remediation. The graphs provided by the solution are unsatisfactory and frequent updates are needed. For instance, suppose you have a specific kernel version of 4.5, and you updated it to version 5.0; the solution still suggests that the older version needs to be fetched and even, in some instances, suggests upgrading to version 5.1. Once the solution implements scans, the records are saved, and a bit of fine-tuning is required for remediation, I have to check manually in a few cases to decrease the number for a few metrics. Sometimes I need to contact the support team to fix bugs. .”

Javeed Abdul

[Read full review](#) 

Senior System Engineer at a tech consulting company with 10,001+ employees

“My main use case for Tenable Cloud Security is managing our security compliance and security posture.

“I use Tenable Cloud Security for managing compliance and security posture, and we rely on the compliance reports and findings of our cloud configuration.

“I don't have anything else to add about my use case or how I use Tenable Cloud Security day-to-day..”

Andrew Lane

[Read full review](#) 

Cloud Security Engineer at a tech vendor with 51-200 employees

“Right now, I use Tenable as CNAPP, and it is good for the product as it offers enhanced security to users. We did use the tool on the cloud. I am not sure if some models, like CIEM, are available as a feature for users. When it comes to a module in CNAPP, I think it is fairly good for using and monitoring on the cloud while also being easy to deploy.

I am not sure how the tool is used in my company because I got transferred to another team that is involved only in monitoring. I use the reporting part on CNAPP. I only use the tool for customized reports. The tool had a fairly easy way to get customized reports..”

Trirong Phuaythip

Solution Consultant at Westcon-Comstor

[Read full review](#) 

“We had other solutions that we used. One solution was that we did not have something exactly similar to what Element is doing. For example, we were using Bitsight, Evelin, and also Tenable Cloud Security. However, those products are different. Element was exactly the product we needed to cover close to real-time external surface monitoring. We also used Microsoft Defender for Endpoint, but the Defender product requires substantial manual labor. We were interested in having a tool that would not require too much manual labor and would be more proactive.

“The Element team is easy to discuss with. They created modules for integrations, such as with DNS. They collect records automatically and add assets to the platform, which is very useful because we do not have to check each day for new records or remove old ones. Their integration with Azure and AWS makes it great for us. It streamlines the process and gives us assurance that all new assets will be automatically added to the platform.

“I am not entirely sure about monitoring cloud applications as I have not used it extensively for that purpose. That is why we implemented Element and have other tools, as we are not using it exactly for that scope..”

DragosCernat

Information Security Architect at WSP

[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 solution's integration and configuration can be overwhelming. If you have a simple environment, I'd rate Tenable Cloud Security's deployment ease very close to ten out of ten. It's easy to deploy, run the first discovery, and manage the assets. Its strength lies in covering the environment thoroughly, discovering assets, and categorizing them..”

Ondrej Kováč

Solution Engineer at Exclusive Networks Czechia

[Read full review](#) 

“The initial setup process is extremely complex; in our company, it has been over a year, and the solution is still being set up. During the setup process in our organization, the tool acquired several vulnerabilities, and I am personally exhausted from managing them. I am personally learning about the competitor solution, HashiCorp Vault, through webinars and trying to compare it with Tenable Cloud Security. A few of my friends are using HashiCorp Vault, and they are comparatively satisfied with the product. .”

Javeed Abdul

Senior System Engineer at a tech consulting company with 10,001+ employees

[Read full review](#) 

Customer Service and Support

“I would rate the tech support a five out of ten. Our company has raised multiple tickets with issues in graphs, but the support team was unable to help. The dashboard of Tenable Cloud Security provides the total number of vulnerabilities instead of segregating them for each day and mentioning how many have been resolved, but there are no useful graphs provided. .”

Javeed Abdul

Senior System Engineer at a tech consulting company with 10,001+ employees

[Read full review](#) 

“Working with Element is straightforward and efficient. For comparison, while working with Bitsight is not difficult, it takes considerably longer. Bitsight is a larger company, and while they will provide the answers needed, the process is more time-consuming. With Bitsight, requesting integrations or new features involves submission and approval processes with uncertain timelines.

“With Element, if you need a feature, you can discuss it with them, and if implementation is possible, you will have that feature within a month or two, depending on complexity. Simple integrations, such as DNS integration, can be completed in approximately a week..”

DragosCernat

Information Security Architect at WSP

[Read full review](#) 

“Our vendor is Broadview, and they offer various support levels. In a typical scenario, with the initial level of support, you might expect a relatively simple approach to problem-solving, with an SLA that allows several hours for issue resolution.

When you open a ticket for a problem, that ticket is overseen by a designated support technical specialist and their manager. If the ticket isn't resolved, you have the option to escalate it through another channel, such as your organization's Cabinet. This process works in a similar way to what we consider normal.

To increase the response speed, you simply need to invest more in advanced support. It doesn't work like it might in smaller vendors. In this context, when there are four tiers of support, each comes with different response times. If you require a one-hour response time, you can opt for premium support, and that's about it. Even before purchasing a solution, whether it's Scalable Security, Account Security, Scalable Security Center, or any other, you can review the support SLAs to gauge how long you might have to wait for assistance with various issues.

.”

Taras Dubrova

BDM at Oberig-it

[Read full review](#) 

Other Advice

“I rate the overall solution a ten out of ten. I think it's the best on the market right now. Other solutions, like Trend Micro, provide incident response across multiple security layers. However, Tenable Cloud Security is not primarily a threat protection tool. Even though it deploys malware detection and removal in the code, it is not like real-time incident response such as Trend Micro..”

Ondrej Kováč

Solution Engineer at Exclusive Networks Czechia

[Read full review](#) 

“My advice to others looking into using Tenable Cloud Security is to go in with expectations around how to manage findings and criticalities and how to manage exceptions. Have an exception process at the ready.

“I don't have any additional thoughts about Tenable Cloud Security before we wrap up.

“On a scale of one to ten, I rate Tenable Cloud Security an eight..”

Andrew Lane

Cloud Security Engineer at a tech vendor with 51-200 employees

[Read full review](#) 

“The solution functions in a multi-cloud environment. In our company, Tenable Cloud Security is implemented in a cloud, but it's connected to the bare-metal data centers. 20% of the solution has been shifted to the cloud environment in our organization, but the tool can still pick data from cloud environments, including

[OCI](#) and [Azure](#). The product efficiently detects vulnerabilities across the entire environment, provides insights, and seeks remediation. Overall, I would rate Tenable Cloud Security a seven out of ten. The solution's vulnerability display interface needs to improve. I recommend others try other competitor solutions and implement a POC before onboarding Tenable Cloud Security. .”

Javeed Abdul

Senior System Engineer at a tech consulting company with 10,001+ employees

[Read full review](#) 

“The tool can be used in the area of vulnerability management to improve our company's security.

I saw some impacts on our finances, especially on the banking side. In our company, we forecast the point for maturity and performance through assessments and security vulnerabilities in the cloud. Before I bought Tenable, I compared it with another band. The tool has been a really good point for the price.

One of the teams in my company would like to use the tool and integrate it with other products used for patching and vulnerability assessment tools.

The tool is a good product that is flexible and on the cloud.

I rate the tool an eight out of ten..”

Trirong Phuaythip

Solution Consultant at Westcon-Comstor

[Read full review](#) 

“Companies are migrating from on-premise to clouds and they must ensure their applications in the cloud will be more safe and secure.

Customers will be more secure in terms of knowing that their applications are running in a safe environment protected by Tenable Cloud Security, so they can promote and extend the migration process to either [GCP](#), [AWS](#), or [Azure](#).

The analytical and reporting capabilities are pretty straightforward and show every transaction and major attempt to attack the application in the cloud. These analytical tools are very complete.

This solution can help organizations adhere to and comply with regulatory requirements such as HIPAA.

On a scale of 1-10, I rate this solution an 8. .”

Antonio Scola

Owner at SUNLIT TECHNOLOGIES

[Read full review](#) 

“[Tenable Cloud Security](#) is a mature and trustworthy product. I have been using it since it was available on laptops approximately 10 years ago or more. I initially used it for penetration testing, though currently I perform more manual penetration testing and use the scanner primarily to validate subnets or findings.

“I started with Nessus installed on my computer, then moved to server deployment, and [finally](#) to Tenable Cloud Security. We still maintain Tenable Cloud Security but have reduced the number of licenses. We now use it occasionally to validate specific items rather than monitoring the entire surface, for which we use Element.

“Tenable Cloud Security offers various features including discovery, web scanning, and primarily vulnerability scanning. It increases awareness of system vulnerabilities. In today's environment, information comes from multiple sources including Defender, Nessus, and various other tools within an organization. Using multiple tools is necessary to cover as much of the attack surface as possible, both internal and external.

“My review rating for the solution is 10 out of 10..”

DragosCernat

Information Security Architect at WSP

[Read full review](#) 

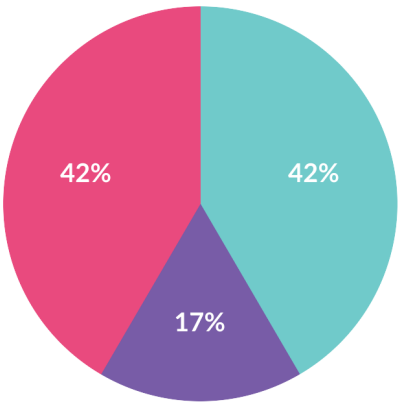
Top Industries

by visitors reading reviews

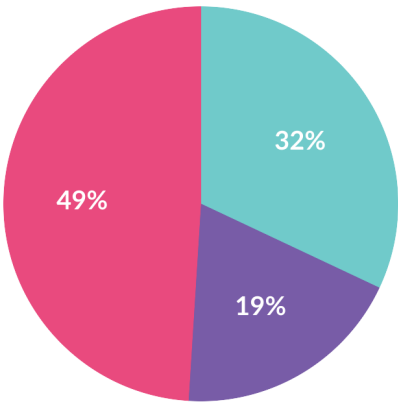


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944