aws marketplace

ThreatModeler Platform

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 10

Other Solutions Considered . . . . . 11 - 13

ROI 14

Use Case . . . . . 15 - 18

Setup 19

Customer Service and Support 20

Other Advice . . . . . 21 - 26

Trends . . . . . 27 - 28

About PeerSpot . . . . . 29 - 30

Product Recap

ThreatModeler Platform

ThreatModeler Platform Recap

ThreatModeler Platform identifies and analyzes potential security risks within applications during development stages, automating threat modeling processes and providing visual threat representations to streamline collaboration.

ThreatModeler Platform is an essential tool for teams focused on aligning security measures with business objectives. It integrates seamlessly into workflows, ensuring comprehensive threat analysis and management. Valued for its automation, collaborative capabilities, and efficient threat visualization, ThreatModeler offers detailed threat diagrams and real-time updates.

What features does ThreatModeler offer?

- **Automation:** Streamlines threat modeling processes to save time and reduce human error
- **Collaboration:** Facilitates cross-departmental cooperation for better security alignment
- **Integration:** Connects seamlessly with other tools used in workflows
- **Drag-and-drop functionalities:** Makes it easy to visualize and manage threats
- **Comprehensive reporting:** Generates detailed reports for in-depth threat analysis
- **Real-time updates:** Ensures threat models are always current and accurate

What benefits should users look for in reviews?

- **Efficiency:** Saves time and effort with automation and streamlined processes
- **Enhanced security:** Provides thorough analysis to protect applications effectively
- **Collaboration:** Promotes teamwork across departments
- **Integration:** Works smoothly with existing tools and workflows
- **Detailed reporting:** Offers valuable insights through comprehensive reports
- **Real-time accuracy:** Keeps threat data up-to-date

ThreatModeler is implemented in industries such as finance, healthcare, and technology, where rigorous security measures are crucial. It supports application development teams in identifying and mitigating potential threats throughout the software lifecycle, ensuring robust protection against cyber incidents.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "ThreatModeler Platform has benefited our team by making the threat modeling process more structured and consistent, with automated threat identification reducing the amount of manual analysis needed for each application and providing a common platform for security and applications teams to review architectural risks and track mitigations, helping us complete initial threat assessments faster and identify issues earlier in the SDLC while enhancing team efficiency and collaboration."

Sasikiran Sakalabattina

Sr Infrastructure engineer at TechMahindra

- "ThreatModeler Platform has positively impacted my organization by changing the approach from manual to a more efficient method, reducing modeling time from 20 hours to just 30 minutes and enabling the team to focus on more important tasks."

Bryan Fearson

Manager, Software Security at Aya Healthcare

"The best features ThreatModeler Platform offers include the enforced threat statement grammar, which requires me to define source, prerequisite, action, impact, and asset for every threat, effectively preventing me from writing vague worries instead of actionable claims."

Leela Aditya Annam

Consultant at a financial services firm with 10,001+ employees

"ThreatModeler Platform has enabled our organization to meet tight delivery dates for product teams by facilitating quick control mapping."

Anusmitha Patnaik

Consultant at HCLSoftware

"ThreatModeler Platform is a big timesaver, helping to provide consistent output. Without it, interpretations would vary. Everything would be developed from scratch, and consistency would be lacking. By having this as our tool, we've developed a more consistent output."

John Thornburg

Sr. Security Architect at a healthcare company with 1,001-5,000 employees

What users had to say about valuable features:

"The customizability is very nice. Unlike a lot of other similar tools, you can build it exactly to your spec. I appreciate the fact that you can iterate on models, so you have the history if you make a change. I can look back on what this exact same model looked like in 2020. The fact that it integrates with our SSO for login is nice as well.."

Bryan Fearson
Manager, Software Security at Aya Healthcare

Read full review

"The best features ThreatModeler Platform offers mainly include data flow representation, which helps identify relevant threats and serves as a good starting point for the assessment. Additionally, control mapping is helpful as it connects identified threats with appropriate security controls.

"ThreatModeler Platform has positively impacted my organization by making it easier to track threats, controls, and overall assessment status. Previously, other platforms were used, but ThreatModeler Platform has unique features that prompted our leadership to adopt it into our practice.."

Anusmitha Patnaik
Consultant at HCLSoftware

Read full review

“ThreatModeler Platform is a big timesaver, helping to provide consistent output. Without it, interpretations would vary. Everything would be developed from scratch, and consistency would be lacking. By having this as our tool, we've developed a more consistent output. It didn't start out that way because everybody has their own ideas, but it is a great tool for making things consistent and making them faster. It allows for drawing solutions to get most of what is needed for threat models, aiding the design team in remediating security requirements.

It measures and mitigates risks across attack surfaces, presents big pictures to leadership, and translates risks into requirements for developers, resulting in security design solutions that save time. Through customization, they can adapt the platform components to match specific needs, significantly streamlining processes..”

John Thornburg

Sr. Security Architect at a healthcare company with 1,001-5,000 employees

Read full review

"The automated threat identification capabilities of ThreatModeler Platform are one of the most useful features for us. It quickly highlights potential risks from the application architecture itself, while the visual modeling of application components, data flows, and trust boundaries makes complex decisions easier to understand. I also find the centralized threat tracking application helpful, as it standardizes threat modeling across different applications instead of relying completely on manual assessments. Its integration with development and security workflows is another strong advantage.

ThreatModeler Platform positively impacts my organization by making application security more proactive and consistent across our development processes. It allows us to identify architectural security risks earlier, preventing significant escalation problems when moving applications into production without addressing vulnerabilities. The automated threat identification reduces manual analysis efforts from the security team, improving collaboration between security, application, and architecture teams. It provides a common view of threats and mitigations of vulnerabilities, ultimately helping us reduce late-stage security findings and making threat modeling a structured part of our SDLC.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

"The best features ThreatModeler Platform offers include the enforced threat statement grammar, which requires me to define source, prerequisite, action, impact, and asset for every threat, effectively preventing me from writing vague worries instead of actionable claims. It acts as a forcing function that keeps my analysis rigorous and consistent. Another standout is the export workflow; unlike many tools that merely produce a static diagram, this platform generates a comprehensive document, including assumptions, data flows, threat statements, mitigations, and other relevant information that my team can actually inherit and act upon. The accessibility is a major benefit, as there is no installation or account requirement, which lowers the barrier between deciding to threat model and actually starting the work. It is a powerful structural vehicle for thinking that does not get in my way, which is why it is so effective for complex cloud-native environments.

"The enforced threat statement grammar fundamentally shifts my workflow from brainstorming to formalizing. By requiring a source, prerequisite, action, impact, and asset for every entry, it forces me to treat each threat as a logical claim rather than a vague worry. This requirement means that by the time I finish the model, I am not just left with a diagram but with a series of defensible arguments that can be evaluated objectively.."

Leela Aditya Annam
Consultant at a financial services firm with 10,001+ employees

Read full review

Other Solutions Considered

"I evaluated other options like Iris Risk before choosing ThreatModeler Platform. The decision was between that and ThreatModeler Platform, which was found to better meet our requirements and our client's needs.."

Anusmitha Patnaik
Consultant at HCLSoftware

Read full review

"Before switching to ThreatModeler Platform, we used Microsoft Threat Modeler, which required a manual approach with limited capabilities. This manual method prompted us to move to ThreatModeler Platform, making our activities significantly easier, and I appreciate my team lead for bringing this solution into our daily tasks.."

Anusmitha Patnaik
Consultant at HCLSoftware

Read full review

"We did not evaluate other options before choosing ThreatModeler Platform. Our previous methods only included manual architecture reviews, which consumed considerable time and resources. Thus, we switched to models like ThreatModeler Platform, standing out due to its combination of visual architecture modeling and automated threat identification, prompting us to adopt this platform.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

"Before ThreatModeler Platform, we primarily handled threat modeling activities using manual architecture reviews, security checklists, and documentation-based assessments. That approach worked well for individual applications but became difficult to scale as our application portfolio grew. For instance, earlier manual architecture reviews wasted two to three hours of time due to increased manual effort. We adopted ThreatModeler Platform to analyze processes and automate initial threat identification, with visible modeling and centralized tagging facilitating collaboration between security and application teams. The transition aimed to make threat modeling more consistent, scalable, reliable, and efficient.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

“Prior to ThreatModeler Platform, threat models were done manually, but this approach was less efficient.

I joined after it was selected, so I wasn't a part of the selection process, but I have evaluated it a couple of times since then and compared it to current products. It seems to be head and shoulders above the rest as far as multi-cloud support. A big thing about it is that we've now integrated it into our work environment such that we can go into and run a report on the security requirements and export them into Jira, and then they can be assigned to a particular team to go through each one of those requirements. They can go through the open ones and fix them. It can automatically, or nearly automatically, be tied into our work environment. It's pretty slick. It's a big time saver. We've integrated it into our platforms. We're doing more and more integration as we go along. A lot of these things didn't exist earlier, at least not to the extent they do now. They've been a result of us working with the ThreatModeling team and them being responsive to our needs.

We initially attempted to port diagrams from draw.io or Visio to ThreatModeler Platform, expecting integration with threat tools. It might have improved now, but at the time, the results were unsatisfactory, leading to manual interpretation and entry processes.

We now get drawings in multiple formats. I'd love to say that we are standardized in the way we should be, but we have multiple teams, and we get multiple formats. We take that drawing and interpret that, and enter it into the tool manually. However, when we are grabbing things, clicking, and dragging them over and making boxes and just sliding things over, as long as the component selection is fairly robust, it's fine. It's a very fast process..”

John Thornburg

Sr. Security Architect at a healthcare company with 1,001-5,000 employees

Read full review

ROI

Real user quotes about their ROI:

"ThreatModeler Platform has reduced training and education costs by enabling security architects to extend their knowledge across various cloud platforms without needing specific certification, leveraging AWS expertise in other environments efficiently.."

John Thornburg Read full review

Sr. Security Architect at a healthcare company with 1,001-5,000 employees

"We primarily see a return on investment through time savings and reduced manual effort. For typical application assessments, automated threat identification saves approximately one to one point five hours compared to manual initial assessments, and sometimes it can save even up to two hours. This helps us identify and fix assessments, enabling earlier resolution of security issues before deployment, minimizing rework during late-stage security reviews. This standardized workflow allows our security team to handle more applications without proportionally increasing manual efforts, resulting in improved efficiency and faster security assessments.."

Sasikiran Sakalabattina Read full review

Sr Infrastructure engineer at TechMahindra

Use Case

"My use case for ThreatModeler Platform is building systems diagrams with a specific focus on the potential threats and security vulnerabilities that could arise should you make a certain change, such as if you connect one server to another server, what are the risks that you could see.."

Bryan Fearson
Manager, Software Security at Aya Healthcare

Read full review

"Our main use case for ThreatModeler Platform is application threat modeling during the design and development life cycle. We use it to analyze the application architecture, data flows, trust boundaries, and potential attack paths. This platform helps to automatically identify security threats based on the application model, allowing us to review and prioritize the findings with the application and security teams. This approach helps us identify and address security risks earlier before the application moves into production.

In a recent application onboarding, we used ThreatModeler Platform to model the applications and data flows, external interfaces, and trust boundaries before they moved towards production. During the assessment, the platform identified potential security risks around an external application component and its communication path to the back-end service. The results and findings with the application and security teams validated the actual architecture, and the team implemented the required access controls and security measures before deployment. This proactive approach helped us identify risks earlier and avoid issues during security testing.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

"My main use case for ThreatModeler Platform involves using it as part of threat modeling activities, where we assess the application architecture to identify potential threats, mapping them to controls, and documenting the overall assessment.

"A specific example of how I used ThreatModeler Platform in a project involves receiving the architecture handbook, going through it, and understanding the architecture diagram. While using ThreatModeler Platform, we draw the Data Flow Diagram (DFD), which helps us assess all potential threats. We double-check the threats and controls it generates with the architecture handbook or connect with our clients to ensure that the controls have been properly mapped. If anything is not mapped, we recommend actions accordingly.

"The use case I have with ThreatModeler Platform has helped to standardize the threat modeling process across different applications, providing a common methodology and documentation. This standardization makes it easier to track threats, controls, and overall assessment status.."

Anusmitha Patnaik
Consultant at HCLSoftware

Read full review

"My primary use case for ThreatModeler Platform is to threat model a complex multi-container environment I designed myself, featuring Open Policy Agent and OPA, and an ABAC-based authorization layer running along Cilium network policies. To test the tool's capabilities thoroughly, I redrew that system as if it were deployed on AWS, incorporating components such as ECS or EKS, ALB, RDS, S3, and Secret Manager with IAM roles scoped individually per service. I built the model directly against that redrawn architecture to ensure I was working with genuine complexity rather than a simplified toy diagram, helping me evaluate the tool's effectiveness in a realistic, high-stakes scenario. ThreatModeler Platform was instrumental in helping me address service isolations and shared secrets, providing a structured way to identify potential vulnerabilities within that specific cloud-native setup. It serves as a perfect test case to see how the tool handles the intricacies of modern containerized infrastructure.

"The real value for me with ThreatModeler Platform is in the enforced grammar of the tool. Because I am modeling a system with complex service isolation and shared secrets, I need a way to ensure my threat statements are consistent. The tool's structure forces me to define the source, prerequisite, action, impact, and asset for every threat, acting as a forcing function for my own thinking. It is not just about drawing a diagram; it is about mapping out the six distinct trust boundaries I identify in that architecture. By forcing me to articulate those boundary crossings, the tool helps me move beyond a high-level overview into much more granular AWS-native analysis. It essentially serves as a vehicle for structured thinking, which is why it is so effective for that specific high-stakes environment.."

Leela Aditya Annam
Consultant at a financial services firm 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 initial setup of ThreatModeler Platform is manageable, and we were able to integrate it into our existing application security workflows without major infrastructure changes. Licensing and pricing are handled by our procurement and vendor management teams, so I do not have direct visibility into contract values or specifics. However, the platform effectively reduces manual modeling effort and streamlines implementation. I would recommend evaluating licenses based on the number of applications, users, and required integrations, as the overall cost is reasonable compared to the security and efficiency benefits.."

Sasikiran Sakalabattina

Sr Infrastructure engineer at TechMahindra

Read full review

Customer Service and Support

"Customer support for ThreatModeler Platform has been very helpful; we have contacted the support team on several occasions and received excellent assistance.."

Anusmitha Patnaik
Consultant at HCLSoftware

Read full review

"We get a very quick initial response. Traditionally, they have been quite fast in resolving issues. We've had a few issues that took a little longer to resolve, and they were resolved in a few days. As a whole, we've had multiple issues because we use the tool all the time and run into problems. They're quick to fix them. Sometimes, we could get a better explanation of what was done to fix it, but all in all, we're happy with the results in the sense that things get resolved quickly. We have somebody who takes our requests and resolves them quickly. Of all the time, all the years that we've had it, we've only had a couple of issues that took a little while longer to resolve.."

John Thornburg
Sr. Security Architect at a healthcare company with 1,001-5,000 employees

Read full review

Other Advice

“We aren't using the governance part yet. I need to look at that more and incorporate that. We aren't using it yet, but it's a good feature. I'd like to find a way to use it. Right now, we're doing governance outside of the tool using other platforms. Maybe we can do it more inside the tool.

I would rate ThreatModeler Platform an eight out of ten..”

John Thornburg
Sr. Security Architect at a healthcare company with 1,001-5,000 employees

Read full review

“I'm not sure that it's significantly impacted our training costs. We use it, but not specifically for training purposes.

We did not notice any changes in application coverage percentages since implementing ThreatModeler since we already had 100% coverage with our applications. We're just more efficient now.

I would recommend ThreatModeler Platform to other users, as it scales and it's the best one that I've seen out there. It just seems the tool that suits the needs of what people who are threat modeling want.

I would rate ThreatModeler Platform an eight out of ten..”

Bryan Fearson
Manager, Software Security at Aya Healthcare

Read full review

“Regarding the export workflow, my team uses those comprehensive documents as a living foundation for security reviews. Because the export includes clear assumptions, data flows, threat statements, mitigations, and open items, it is something a reviewer can actually interrogate line by line rather than just a picture.

“I would frame ThreatModeler Platform's impact not as organizational transformation but as workflow impact. Since my hands-on use has been focused and recent rather than a long-term deployment across a team, the clearest gain is speed to a usable output. Before, building a threat model meant starting from a blank diagram and hoping the resulting document held together. With ThreatModeler Platform, the enforced grammar regarding threat source and prerequisite, action, impact, and asset means every entry survives being stated as a real claim rather than a vague concern. That structure alone cuts the time from needing to think about security to having a reviewable artifact significantly. It also improves the quality of the review itself because the output is structured. With assumptions, data flows, threat statements, mitigations, and open items, it is something a reviewer can actually interrogate line by line.

“I rate ThreatModeler Platform an eight out of ten because AWS-native modeling with a real reviewable export for free is valuable. It loses points only for manual diagramming and no infrastructure-as-code sync, which is a genuine limitation and not a nitpick. Eight reflects strong execution with one honest, unresolved gap..”

Leela Aditya Annam
Consultant at a financial services firm with 10,001+ employees

Read full review

“I recognize various AI controls that enhance our processes. The AIML-related features significantly assist in drawing data flow diagrams, benefiting our organization's governance practices.

"ThreatModeler Platform is deployed in our organization on a private cloud, and we can access it only after logging into the VDI.

"Customizing Threat Framework components in ThreatModeler Platform to match our company needs involves some challenges, but there are various components available. We can search for specific items, and if matching stencils are unavailable, we can use general components or place items out of scope as needed while creating the data flow diagram.

"Regarding whether ThreatModeler Platform has helped our security team keep pace with DevOps sprints, I cannot assure this because I have not seen it in our current practice.

"I can confirm that ThreatModeler Platform has reduced the hours needed to complete threat modeling projects, as we now complete assessments within half the time, going from three to four weeks down to just one or two weeks.

"After implementing ThreatModeler Platform, we have observed improvements in application coverage percentages. When we identify existing gaps through assessments, we collaborate with the development team to address them, allowing us to produce comprehensive assessments once fixes are applied.

"ThreatModeler Platform has enabled our organization to meet tight delivery dates for product teams by facilitating quick control mapping. There have been instances where clients required threat modeling during their deployment stage, and ThreatModeler Platform helped us expedite the process by allowing us to map controls efficiently, even when multiple cases needed to be processed simultaneously.

"I would recommend ThreatModeler Platform to organizations looking to establish a structured and repeatable threat modeling process, as it reduces manual efforts and ensures consistency, although it is essential for experienced security analysts to validate the generated threats and controls. I give ThreatModeler Platform a rating of ten out of ten.."

Anusmitha Patnaik
Consultant at HCLSoftware

Read full review

"ThreatModeler Platform fits into our workflow mainly during the application design and security review stage. We use it before production deployment to understand the application architecture, data flows, trust boundaries, and potential threats. The security team generates findings with the application and architecture teams and tracks the required mitigations. It complements our vulnerability scanning and other security testing rather than replacing them, helping us shift security assessments earlier in the SDLC and providing a more consistent threat modeling process.

The automated threat identification feature has made our process more efficient by providing a quick initial assessment of potential threats. Instead of relying solely on manual analysis, once we build the application model, ThreatModeler Platform identifies relevant threats based on the architecture and data flows. This allows our security team to focus more on validating findings and collaborating with developers on mitigation. It also ensures a consistent approach across different applications, overall reducing manual analysis efforts and helping us identify security risks earlier in the development lifecycle.

One feature I particularly value is the combination of visual threat modeling and threat identification, which makes complex application architecture easier for both security and development teams to understand. The centralized tracking of threats and mitigations also improves collaboration and follow-up. Version seven point five provides a smoother experience compared to older versions like seven and seven point two, making features more consistent and preferable in our approach to application security.

In our hybrid cloud environment, we primarily utilize Microsoft Azure alongside our own on-premises infrastructure. ThreatModeler Platform is integrated into our application security workflow across both environments before deployment. These threat models help us maintain consistent security reviews based on both on-prem and Azure-hosted applications, which is particularly useful when applications have dependencies across both environments.

ThreatModeler Platform is deployed as part of our application security and threat modeling workflow. We have been using this platform for around three years,

initially with version seven and currently with version seven point five. Security and application teams access the platform to create and maintain threat models for the application during design and review stages, considering components, data flows, trust boundaries, and external interfaces. The platform serves as our centralized threat modeling solution in a hybrid cloud environment.

ThreatModeler Platform helps us assess risks across different application attack surfaces in a structured way. We model components such as internet-facing interfaces, APIs, authentication points, data stores, and back-end services, along with the data flows between them. The platform assists in identifying threats associated with those components and trust boundaries. We review findings with application and security teams, prioritizing applicable risks for mitigation, giving us better visibility into the overall attack surface rather than considering individual components in isolation.

ThreatModeler Platform has indeed helped our security team keep pace with DevOps sprints by integrating threat modeling earlier into the application development processes. For instance, when application architecture or APIs change during a sprint, we can utilize the platform to update the threat model and quickly review newly identified risks. Automated threat identification reduces the time required for initial security assessments, allowing security and development teams to focus on validating relevant findings and tracking remediation. This integration helps avoid making threat modeling a separate activity that delays sprint production releases.

We primarily see a return on investment through time savings and reduced manual effort. For typical application assessments, automated threat identification saves approximately one to one and half hours compared to manual initial assessments, and sometimes it can save even up to two hours. This helps us identify and fix assessments, enabling earlier resolution of security issues before deployment, minimizing rework during late-stage security reviews. This standardized workflow allows our security team to handle more applications without proportionally increasing manual efforts, resulting in improved efficiency and faster security assessments.

The flexibility to automate specific parts of our threat modeling process with ThreatModeler Platform reduces repetitive manual training necessary for day-to-day assessments. Once we establish a standard modeling workflow, team members can follow a consistent approach rather than learning different methods for every application. While new team members still require training on ThreatModeler Platform and threat modeling, the standardized workflow simplifies onboarding. I did not measure a specific percentage reduction in training costs, but the primary benefit lies in less training effort and faster onboarding.

ThreatModeler Platform enables our organization to meet tight delivery dates for product teams by providing quick initial assessments through automated threat identification. This feature is invaluable when an application has a short release window. We can swiftly review the architecture, validate, generate threads, and focus solely on the high-priority areas on the list to reduce security review delays, allowing application teams to address issues promptly before the release. It is especially useful when multiple applications require security assessments within the same delivery cycle.

ThreatModeler Platform has benefited our team by making the threat modeling process more structured and consistent. Automated threat identification reduces the amount of manual analysis needed for each application, providing a common platform for security and applications teams to review architectural risks and track mitigations. In practice, it helps us complete the initial threat assessments faster and identify issues earlier in the SDLC. Overall, this improvement enhances team efficiency and collaboration without eliminating the need for technical validation. I rate my overall experience with ThreatModeler Platform as nine out of ten.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

Top Industries

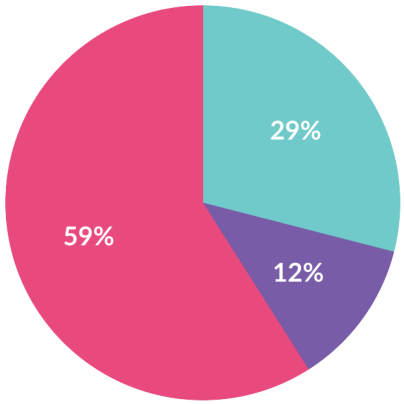
by visitors reading reviews

Financial Services Firm	23%
Wholesaler/Distributor	10%
Manufacturing Company	8%
Mining And Metals 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