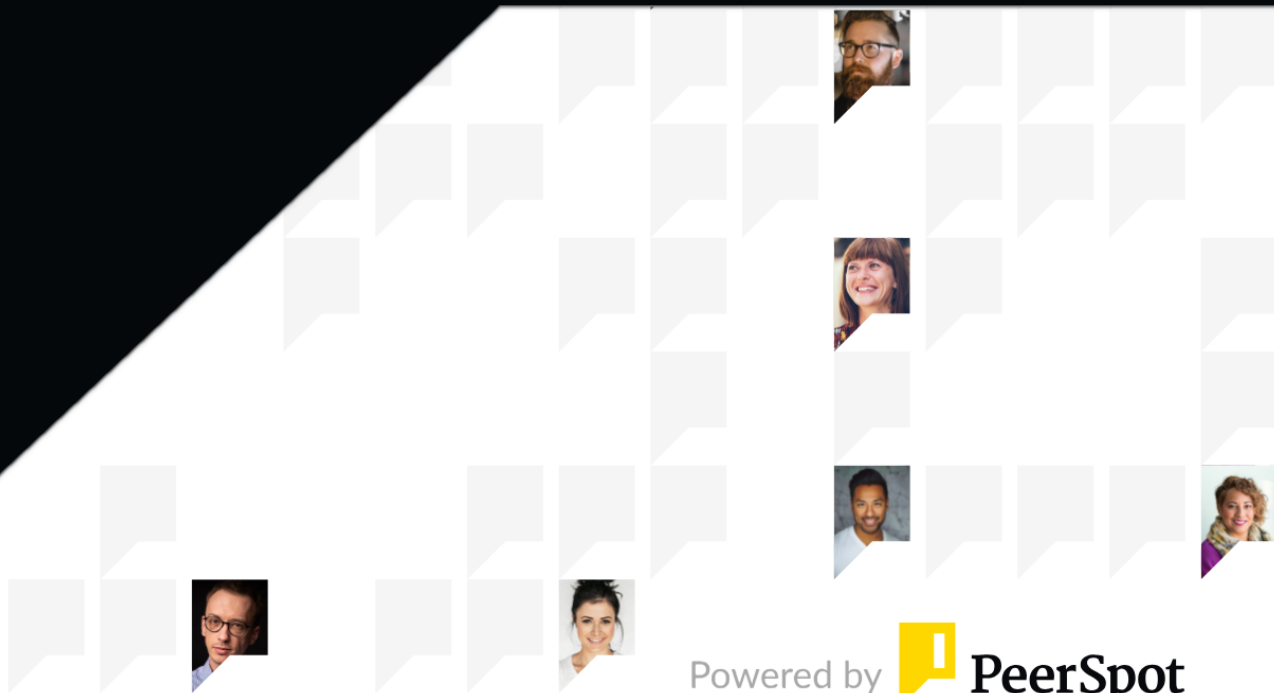


aws marketplace

AttackIQ

**Reviews, tips, and
advice from real users**



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13

ROI..... 14 - 15

Use Case..... 16 - 20

Setup..... 21 - 22

Customer Service and Support..... 23 - 24

Other Advice..... 25 - 27

Trends..... 28 - 29

About PeerSpot..... 30 - 31

Product Recap



AttackIQ

AttackIQ Recap

AttackIQ offers a cybersecurity platform focusing on security optimization through breach and attack simulation, enabling organizations to assess and improve their defense mechanisms effectively.

Using advanced technology, AttackIQ helps organizations evaluate security processes against real-world threat scenarios. Its platform provides continuous security assessments, which help in identifying vulnerabilities before exploitation by adversaries. It allows for the strategic allocation of resources towards enhancing security through actionable insights and reporting.

What key features make AttackIQ stand out?

- **Breach and Attack Simulation:** Conducts realistic attack scenarios to test defenses.
- **Automated Testing:** Regularly checks security protocols against evolving threats.
- **Comprehensive Reporting:** Offers detailed insights into security performance metrics.
- **Threat Intelligence Integration:** Incorporates global threat data for precise assessments.

What benefits and ROI should be evaluated?

- **Improved Security Posture:** Leads to a reduction in potential system breaches.
- **Resource Optimization:** Allows allocation of resources to high-risk areas.
- **Enhanced Awareness:** Increases understanding of threat landscapes within teams.
- **Risk Mitigation:** Identifies weaknesses before they result in data leaks.

Industries such as finance and healthcare, highly sensitive to data breaches, utilize AttackIQ for its rigorous testing capabilities. By simulating sophisticated cyber threats, organizations within these sectors can better protect critical data and maintain compliance with stringent regulatory standards.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Running in our SOC, it moves the conversation from assumptions and dashboards to measurable proof, which is exactly what makes AttackIQ valuable in day-to-day security operations.”



Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees



“AttackIQ has had a positive impact on the organization, especially in the areas of continuous security validation, detection improvement, and overall defensive readiness, with highlights including improved visibility into detection gaps, stronger security controls validation, better SOC readiness, and faster detection engineering improvements, which are improvement areas we have implemented in our project using AttackIQ.”

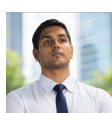


SangramGupta

Security Consultant at Deloitte



“AttackIQ has improved my security posture by validating security controls, identifying detection gaps, and increasing confidence in my detection and response capabilities.”



Mukul Gosavi

SOC L2 | Incident Responder at a financial services firm with 501-1,000 employees



“AttackIQ is solving a lot of the problems that I had before or that we as an organization had before, even the security team, so it is solving all my issues.”



Verified user

DevOps at a marketing services firm with 51-200 employees



“After using AttackIQ, it has helped the team and the company improve on false positives and reduce risk, as most people are now capable of identifying how to work on detection, improving fine-tuning and all those things.”



Verified user

Software Development Analyst at a tech vendor with 10,001+ employees



“Overall, I've had a good experience with the product. It's worked well for me.”



NOUBOUM NOUBI BORIS HERMAN

Network Performance Management at Huawei Cameroun

What users had to say about valuable features:

“The continuous testing and continuous offensive testing are among the best features that AttackIQ offers, and being able to categorize it based on criticality such as very critical, emergency, high, medium, and low is valuable.

AttackIQ allows us to resolve issues much quicker because these issues come in categories, enabling us to prioritize them and fix the emergency issues first.

It has definitely reduced response time and improved our discoverability of these issues in the first place..”

Verified user

[Read full review](#) 

DevOps at a marketing services firm with 51-200 employees

“The best features AttackIQ offers include MITRE ATT&CK mapping, automated breach simulations, security control validations, detection gap analysis, and detailed reporting.

“AttackIQ has improved my security posture by validating security controls, identifying detection gaps, and increasing confidence in my detection and response capabilities.

“The feature I rely on most is security control validation. It gives me confidence that my security controls and detection mechanisms are working as expected against real-world attack techniques. Instead of assuming my defenses are effective, I can validate them regularly, identify gaps, and fine-tune my security tools before an actual incident occurs. I was impressed by the MITRE ATT&CK-based simulations and the depth of the reporting..”

Mukul Gosavi

SOC L2 | Incident Responder at a financial services firm with 501-1,000 employees

[Read full review](#) 

“I would say that the features of AttackIQ I find most valuable are its ease of use and the integration with security tools. It adds a lot of value for the customer when it can be integrated with their ecosystem to be tracked, so with the customer having multiple security tools in place, the integration helps a lot.

The integration with security tools helped my customers because the platform itself does the scanning, and as continuous scanning occurs, any deviation from the standard happens. We can either pull the logs or pull the alerts via API, or it can be exported depending on what kind of SOC tool that you use. That particular alerting mechanism is critical when it comes down to making sure that the operations are working as expected. I appreciate that feature.

AttackIQ has positively impacted my organization and my customers by making it easier for them to validate their configurations all the time when it is not easy to do so. Anyone can make a small mistake. Exposure management, as it does continuous scanning all the time, reduces the time of detection of any configuration errors or something unwanted exposed over time. It helps a lot because what I have seen is that most of the time, misconfigurations lead to catastrophes. AttackIQ helps with that..”

Verified user

[Read full review](#) 

Professional Services Engineer at a tech services company with 201-500 employees

“The best features AttackIQ offers include being a cybersecurity platform specializing in breach attack simulation and AEF validation, as it tests the organization's defenses by simulating real-world attack behavior, which are aligned with the MITRE ATT&CK framework, providing a platform where I can run real-world attack scenarios and identify and mitigate them.

“AttackIQ is well-aligned with the MITRE ATT&CK framework and has strong continuous validation. The platform is built to run continuous and automation tests, which helps during point-in-time checks or reduces blind spots.

“AttackIQ positively impacts my organization as most of my colleagues and seniors have been using it to understand real-world attack scenarios and how to cope with those situations, benefiting the company, colleagues, and team.

“After using AttackIQ, it has helped the team and the company improve on false positives and reduce risk, as most people are now capable of identifying how to work on detection, improving fine-tuning and all those things. It has definitely benefited the organization in terms of faster risk identification and faster response times..”

Verified user

[Read full review](#) 

Software Development Analyst at a tech vendor with 10,001+ employees

“Some of the best features I found in AttackIQ are its continuous security validation capabilities, MITRE ATT&CK alignment, and the ability to proactively test whether security controls are actually working as expected in real-world attack scenarios, representing real-world case studies and best features I have encountered in my project.

The continuous security validation capabilities of AttackIQ were one of the most valuable parts used by our team, especially since before using the platform, a lot of validation activities depended on periodic penetration testing, manual testing, or assumptions that security controls are functioning, which presented an actual challenge for the overall organization. AttackIQ helped change that, making validation more operational, repeatable, and proactive. From a usability perspective, once the initial setup and workflows are configured, the platform becomes fairly straightforward for day-to-day validation activities, with MITRE ATT&CK mapping and predefined attack scenarios making it easier for security teams to understand what was being tested and how the controls were responding.

AttackIQ has had a positive impact on the organization, especially in the areas of continuous security validation, detection improvement, and overall defensive readiness, with highlights including improved visibility into detection gaps, stronger security controls validation, better SOC readiness, and faster detection engineering improvements, which are improvement areas we have implemented in our project using AttackIQ.

The overall detection has actually improved with AttackIQ, as the SOC improved, which reduced a lot of false positives and increased the detection rate and accuracy. Previously, a lot of time was consumed to detect something or to conduct false positive investigations, but after implementing AttackIQ, there is now a reduction of almost 40 to 50% in the overall time and effort, making it an impactful area..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“Running in our SOC, it moves the conversation from assumptions and dashboards to measurable proof, which is exactly what makes AttackIQ valuable in day-to-day security operations.

The breach and attack simulation that supports testing, prevention, detection, and response is a key feature for me, as is the ongoing exposure management, rather than a one-time security assessment. AttackIQ's reporting helps translate technical findings into actionable remediation steps, which are easy to understand. The continuous validation of security controls through repeatable attack simulations is a massive advantage for me.

Once properly implemented, AttackIQ becomes a valuable part of a continuous validation program.

The one feature I rely on the most from AttackIQ is specifically the continuous validation of security controls through repeatable attack simulations. From the reporting that stands out, once you have the report, the translation from a technical finding perspective and how they align with actionable remediation steps is easy to understand, which helps significantly.

From a SOC perspective, AttackIQ running in our SOC is a solid enterprise-grade platform delivering genuine operational value. The biggest strength for me is the realism, its alignment with all the compliance situations we might have, and the ability to continuously validate control effectiveness. By doing that, we can continuously provide feedback to our customers to ensure they are running the best of breed for their security posture and environment. AttackIQ is best viewed as a tool that helps a SOC move from assumption-based security to evidence-based security, while providing reporting that can easily be communicated in layman's terms to your customer base. It is most effective for teams that want to prove their controls work, identify gaps early, and continuously improve rather than just rely on periodic testing alone..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

Other Solutions Considered

“I have tested other solutions as well, and AttackIQ is the platform I used. I chose to switch to AttackIQ because of the integration that they provide..”

Verified user

Professional Services Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“Previously, we did use a different solution. However, I am not going to say which solution it was, but we switched because of the difficulty in integrations, as the reporting was quite disorganized, difficult to understand, and difficult to really articulate back into layman's terms. The cost was excessive..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“It's hard to say about money saved because it has only been four and a half months with AttackIQ, but definitely a lot of time has been saved. I would say approximately 15% of our time..”

Verified user

[Read full review](#) 

DevOps at a marketing services firm with 51-200 employees

“We have seen a massive return on investment with AttackIQ, specifically from a resource perspective and time spent on findings due to the fact that the accuracy of the reporting or the accuracy of the findings from AttackIQ was brilliant. This saves a lot of manpower time..”

Charl Pinches

[Read full review](#) 

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

“I have definitely seen a return on investment from AttackIQ. Time saved is evident. I may have to connect back to the customer to figure out whether it has reduced the number of incidents, but time saved for configuration mistakes and those kinds of things is definitely positive..”

Verified user

Professional Services Engineer at a tech services company with 201-500 employees

[Read full review](#) 

Use Case

“My main use case for AttackIQ is conducting breach and attack simulation or any kind of new ransomware simulation, basically for executing particular real-world attack scenarios.

“Regarding my main use case, I have used AttackIQ Ready, Flex, and Enterprise, which are the main three product types I have utilized most..”

Verified user[Read full review](#) 

Software Development Analyst at a tech vendor with 10,001+ employees

“We use AttackIQ for automated, continuous testing and offensive testing. We use their scaled offensive testing module in AttackIQ, which continuously validates your environment and cloud environment, then identifies exposures that we take and try to fix them.

I'm the security person on the team, so AttackIQ has become really useful for us to automate this continuous testing because before we would only have point-in-time testing. We would only be able to get a scan at a single point in time, but now it's useful because it provides continuous monitoring.

We use public cloud for AttackIQ..”

Verified user[Read full review](#) 

DevOps at a marketing services firm with 51-200 employees

“I use AttackIQ primarily as part of security validation and threat exposure assessment within our cybersecurity operation, where the platform is mainly used to simulate attack techniques and validate whether the existing security controls are effectively detecting and responding to the threats.

We conducted a purple team exercise where we used AttackIQ to simulate attack behaviors mapped to MITRE ATT&CK techniques with the control testing environment, with the main goal being to validate whether the SIEM detection was triggering correctly and to check if the endpoint security controls are responding as expected, and if the SOC monitoring workflows were functioning properly. That exercise helped identify a few detection gaps where certain behaviors were either not generating alerts consistently or lacked sufficient contextual visibility, and based on the findings, the security team refined the SIEM correlation rules, improved the alert prioritization, and enhanced monitoring coverage for specific attack techniques..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“My main use case for AttackIQ is security control and validation, breach and attack simulations, detection validation, and security posture assessment.

“I used AttackIQ to simulate MITRE ATT&CK techniques such as phishing related credential access and lateral movement to verify whether Microsoft Defender for Endpoint and our SIEM generated the expected alerts. I reviewed any detection gaps, fine-tuned detection rules, and reran the assessment to confirm the improvements.

“My primary focus was validating the effectiveness of our existing security controls rather than just checking compliance. AttackIQ helped me to identify detection gaps, verify the security tools were working as expected after policy changes, and improve my responses by safely simulating real-world attack tactics..”

Mukul Gosavi

SOC L2 | Incident Responder at a financial services firm with 501-1,000 employees

[Read full review](#) 

“Basically, I use AttackIQ for exposure management where I have customers who want attack surface validation on their risk profile and cyber exposures. I have used it in a couple of places where the customer entities were scanned all the time. They wanted it to be scanned to make sure that there are no misconfigurations.

A specific example of how I used AttackIQ for exposure management is with a customer who has many services hosted on top of AWS instances. These are a mix of PaaS and SaaS platforms. Because the development team is separate and the infrastructure management team is separate, the developers wanted visibility on what things are exposed from the development side as well as from the production side, and they wanted to validate that. There was a use case from the infrastructure side regarding whether there are any misconfigurations or open ports. They did not want to be exposed to scanning continuously and wanted it to be reported. AttackIQ helped and worked closely with the CSO to come up with a plan.

The main use case is for exposure management, but I understand that there are other verticals as far as AttackIQ is concerned, but that is the one that I have used it for..”

Verified user

Professional Services Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“The key features that we mainly depend on are the continuous validation of security controls through repeatable attack simulations. Whenever there's a breach or attack simulation happening, the support, testing, preventing, detection, and response behind it is completely ongoing.

At the same time, exposure management, rather than just a one-time security assessment, helps us to stay on top of what's happening in the environment and reduces fatigue for a SOC engineer or someone managing the SOC to find the actual attack entrance, the problem behind it, or how the breach might have taken place.

From a SOC perspective, AttackIQ gives us clear evidence of where the controls are working in real conditions and is practically strong for identifying detection gaps and response weaknesses. Being aligned with MITRE ATT&CKs makes it easier to prioritize and communicate our findings back to our clients running in our SOC.

There are several use cases for how we use AttackIQ in our SOC. It is most useful for validating detection coverage, testing response readiness, and confirming whether endpoint and security controls behave as expected. It is also a strong fit for post-deployment validation after introducing new tooling because it helps prove whether the changes actually improve the security posture. AttackIQ works particularly well with ransomware simulations, exposure management programs, and recurring control assessments. For my team that wants to measure defensive capability over time, it provides a structured and repeatable way to do that..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 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 rollout process is quite easy to do because we have a mature SOC team and engineers around it. The understanding process on how to get all of this to tie back into an existing mature SOC took some challenges, but it was easily resolved..”

Charl Pinches

[Read full review](#) 

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

“One area for improvement is the initial configuration complexity, which is very complex in the initial stage to configure the whole thing and integrate with the SOC, presenting a learning curve for organizations that are new to adversary emulation or continuous security validation..”

SangramGupta

[Read full review](#) 

Security Consultant at Deloitte

“The initial setup was difficult. It was not straightforward. I struggled at the outset to get everything up and running.

The deployment itself took a long time to execute on.

The product does require regular maintenance as well..”

NOUBOUM NOUBI BORIS HERMAN

Network Performance Management at Huawei Cameroun

[Read full review](#) 

Customer Service and Support

“Overall, my experience with the customer support of AttackIQ has been positive, with the support team generally responsive, technically knowledgeable, and helpful during both onboarding and operational phases..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“I haven't had any issues with the product just yet. Therefore, I haven't reached out to technical support before. Having not spoken to them, it's hard for me to gauge their level of knowledge or responsiveness. I wouldn't be able to really comment..”

NOUBOUM NOUBI BORIS HERMAN

Network Performance Management at Huawei Cameroun

[Read full review](#) 

“AttackIQ's customer support is brilliant.

I have not needed customer support too many times, but from the times we have had instances where we needed customer support, I would rate it an eight out of 10..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

Other Advice

“My advice for others looking into using AttackIQ is that it is a good product. Configure the scans the way you want them, but make sure that you are not too aggressive with the scanning. I would rate this product a nine out of ten..”

Verified user

Professional Services Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“I suggest defining clear use cases, integrating AttackIQ with your security tools, and running simulations regularly. AttackIQ is a strong platform for security validations. Better integration, AI-driven remediations, and customizable reporting would make it even better. I would rate this product an 8 out of 10..”

Mukul Gosavi

SOC L2 | Incident Responder at a financial services firm with 501-1,000 employees

[Read full review](#) 

“I would rate AttackIQ a 10 out of 10 because so far I have no issues with it. AttackIQ is solving a lot of the problems that I had before or that we as an organization had before, even the security team, so it's solving all my issues. I would say definitely make sure you know your use case before you purchase AttackIQ. I give this product a rating of 10 out of 10..”

Verified user

DevOps at a marketing services firm with 51-200 employees

[Read full review](#) 

“The accuracy of AttackIQ is very good and the reliable output is straightforward and easy to understand.

The advice I would give to others looking into using AttackIQ is to make sure that your SOC already has a process for acting on findings and that the SOC is mature enough to handle AttackIQ. I rate this review a 9 out of 10..”

Charl Pinches

Solutions Sales Specialist at a outsourcing company with 1,001-5,000 employees

[Read full review](#) 

“One additional point I would like to add is that we will improve continuous security validation. Traditionally, many organizations rely heavily on periodic penetration tests or isolated assessments to evaluate security effectiveness, while AttackIQ helped us achieve a more continuous and operational approach to security controls, detections, and monitoring workflows, actually working as intended over time. We are the customer. I would rate this product a 7 out of 10..”

SangramGupta

Security Consultant at Deloitte

[Read full review](#) 

“In my current organization, we are not using AttackIQ; in my previous organization, I have used AttackIQ, and it was more of hands-on training rather than being deployed as a typical tool for improvement or knowledge enhancement.

“In my previous experience with AttackIQ, it was all on-premises and training; we have not used any private cloud vendor.

“My advice for others considering using AttackIQ is that people can utilize it since it offers free training on purple teaming and pre-simulation, which are useful for professional growth and skills development, even for those with limited industry certifications. I would rate this review an eight out of ten..”

Verified user

Software Development Analyst at a tech vendor with 10,001+ employees

[Read full review](#) 

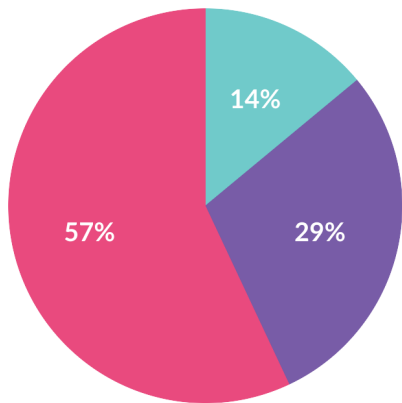
Top Industries

by visitors reading reviews

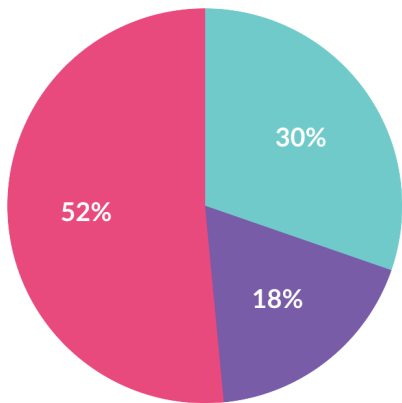


Company Size

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