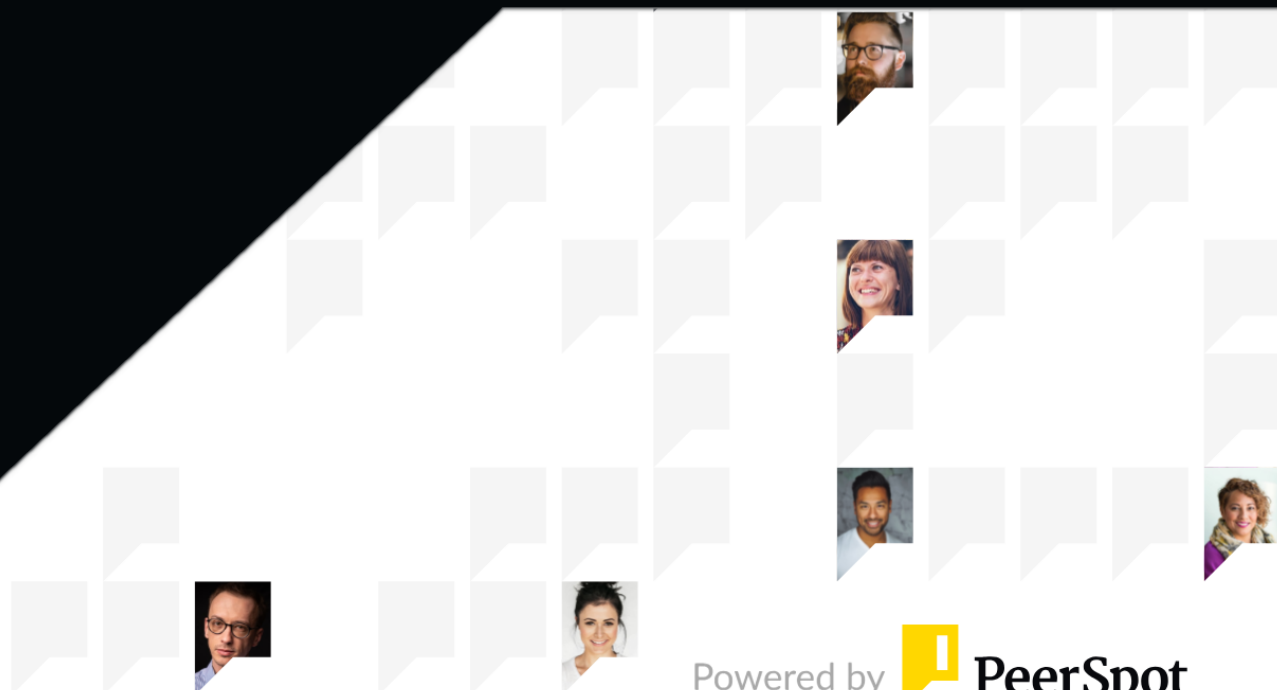




Arctic Wolf Managed Detection and Response

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 9

Other Solutions Considered..... 10 - 11

ROI..... 12 - 14

Use Case..... 15 - 17

Setup..... 18 - 21

Customer Service and Support..... 22 - 24

Other Advice..... 25 - 27

Trends..... 28 - 29

About PeerSpot..... 30 - 31

Product Recap



Arctic Wolf Managed Detection and Response

Arctic Wolf Managed Detection and Response Recap

Built on the industry's only cloud-native platform to deliver security operations as a concierge service, the Arctic Wolf® Managed Detection and Response (MDR) solution eliminates alert fatigue and false positives to promote a faster response with detection and response capabilities tailored to the specific needs of your organization. Your Arctic Wolf Concierge Security® Team (CST) works directly with you to perform threat hunting, incident response, and guided remediation, while also providing strategic recommendations uniquely customized for your environment.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“The asset scanning feature and the entire solution, especially their advanced threat protection recently released, are very effective.”



Kimberly Brock

Technical Security Engineer & Data Governance at a computer software company with 51-200 employees



“The solution works well for our team as it offers a hands-off approach, which we need.”



Adrian Cambridge

Head of IT at AHMM



“The tool definitely saves money for our company's customers.”



Daniele Brommer

Commerical Manager at Network Service Providers Limited



“The most valuable aspect of this solution is the managed detection and response component.”



Jared Kruger

Buisness Developer Manager / Sales Executive at Troye



“The product provides integrations with several different SaaS applications.”



Verified user

Group Manager, Information Technology Security at a manufacturing company with 1,001-5,000 employees



“The visibility into our endpoints is huge.”



Verified user

Director of IT Operations at Planalytics, Inc.



“We can effectively manage the massive amounts of security data that we receive from various sources such as firewalls, switches, endpoints, and other log sources.”



Todd Lienke

Vice President of Technology at Hallmark Building Supplies, Inc.

What users had to say about valuable features:

“The solution works well for our team as it offers a hands-off approach, which we need. The pricing is okay and comparable to other solutions. We value the hands-off approach as we don't have our own security team. We have monthly meetings with them, where they help us secure parts of our network, which is valuable to us..”

Adrian Cambridge

Head of IT at AHMM

[Read full review](#) 

“The agents that are installed help detect threats. The agents give pretty good visibility into what is happening at the endpoint. The response to threats is pretty quick. Depending on the severity, the team sends an email or gives us a direct call. The weekly and monthly reports through the dashboard are helpful..”

Verified user

Service Security Analyst at a government with 11-50 employees

[Read full review](#) 

“The solution's most valuable feature is the certainty that someone is watching it, and that is the one key thing that I love about the product. Apart from the tool's own local team, somebody is always watching the tool and reducing any risks. The awareness training and all that stuff are good because Arctic Wolf Managed Detection and Response does it all by building such areas..”

Daniele Brommer

Commerical Manager at Network Service Providers Limited

[Read full review](#) 

“The most valuable aspect of this solution, both for me and my clients, is the managed detection and response component, which is a core feature of the service. However, what sets it apart is the "concierge security team" that provides customers with two dedicated resources for proactive security management. This personalized support, in addition to the 24/7 SOC service, is a significant added benefit..”

Jared Kruger

Buisness Developer Manager / Sales Executive at Troye


[Read full review](#) 

“Their asset scanning features are a game changer. The entire solution, especially their advanced threat protection recently released, are very effective in helping to mitigate corporate risks. The concierge team is excellent. The Arctic Wolf agents, which are constantly performing scans help to produce almost real-time reporting.

Threat detection is remarkable. Security is everyone's responsibility and Arctic Wolf does an excellent job ensuring the company is trained, sending out timely videos about industry happenings. Their educational materials are invaluable. The content they release is timely, and employee engagement is notably high..”

Kimberly Brock

Technical Security Engineer & Data Governance at a computer software company with 51-200 employees

[Read full review](#) 

“The visibility into our endpoints is huge.

The data collected is provided in a view that is understandable and approachable.

The quarterly review with our account manager and Concierge Security Team provides good information and also provides a nice overview of the Arctic Wolf roadmap.

The Security Bulletins that Arctic Wolf provides when there is a new threat or zero-day vulnerability are extremely helpful. They explain the issue and provide understandable recommendations with actionable steps..”

Verified user

Director of IT Operations at Planalytics, Inc.

[Read full review](#) 

Other Solutions Considered

“We were using a product from a local Danish vendor. We switched to Arctic Wolf Managed Detection and Response for cost and capabilities. It offered more features and better support, including superior threat intelligence feeds. .”

Verified user

security lead at a legal firm with 201-500 employees

[Read full review](#) 

“While we have used an antivirus previously, we haven't used anything quite like Arctic Wolf. We chose Arctic Wolf as it integrated with our antivirus and had a strong global presence. .”

Verified user

AVP of Tech at a insurance company with 201-500 employees

[Read full review](#) 

“We have discussed their use of AI in learning modules; however, it is not yet heavily integrated into their decision-making processes. While AI may exist in the product to some extent, it does not perform the role of a security engineer..”

Kimberly Brock

Technical Security Engineer & Data Governance at a computer software company with 51-200 employees

[Read full review](#) 

“I did not choose this solution. I came into the company and this product was already here. I will say that I have removed a number of products from our vendor list during my first year, and have not considered removing Arctic Wolf – despite it being one of our costlier contracts. .”

Verified user

[Read full review](#) 

Director, IT Systems and Security at Union Mutual Fire Insurance Company


“We use both Artic Wolf Managed Detection and Response and Artic Wolf Managed Risk.

I have been using Artic Wolf Managed Risk for a little over a year.

We are working with the latest version.

We offer two products: one specifically designed for managing network security, and the other for providing training to your associates..”

Todd Lienke

[Read full review](#) 

Vice President of Technology at Hallmark Building Supplies, Inc.

ROI

Real user quotes about their ROI:

“The ROI is keeping our business up and running. We have not been down, nor have we had any ransomware attacks or any intrusion into our network in the past three years..”

Verified user

[Read full review](#) 

AVP of Tech at a insurance company with 201-500 employees

“Considering the number of activities that customers have to indulge in, especially with the increase in attacks in New Zealand, I can say that the tool helps save a time frame of seven days..”

Daniele Brommer

[Read full review](#) 

Commerical Manager at Network Service Providers Limited

“I am beginning to see the return on investment because the tool saves me resources. On average, we get a 50% return on investment. We can't completely do away with your SOC team. However, I don't have to hire more people as I scale up. The solution's service runs 24/7. It definitely takes a load off of me. I do not need a team 24/7..”


Verified user

[Read full review](#) 

Group Manager, Information Technology Security at a manufacturing company with 1,001-5,000 employees

“Calculating the return on investment can be challenging in this type of scenario because ideally, you don't want to experience any security incidents that would require the use of the service. It's similar to insurance in that it's something you pay for but hope to never have to use..”

Todd Lienke

[Read full review](#) 

Vice President of Technology at Hallmark Building Supplies, Inc.

“It is hard to calculate the ROI when dealing with most cyber security items as if threats don't get you, you don't really know about them. They've been there when we needed them. As far as I'm concerned, this is money well spent. Plus, we didn't have to go out and get our own SIEM and find someone to manage it. .”

Verified user

[Read full review](#) 

CIO at Professional Services Organization in Washington DC Area

“The services provided by Arctic Wolf are comprehensive. Their training materials and videos benefit the organization as a whole. While similar training is available from other companies, Arctic Wolf's offerings are timely and effective. Employee engagement is high, with a 96% viewing and participation rate for their training materials. The company has achieved strong cultural buy-in..”

Kimberly Brock

Technical Security Engineer & Data Governance at a computer software company with 51-200 employees

[Read full review](#) 

Use Case

“We use them as our managed doc. Instead of hiring a security specialist, we'd rather pay for a solution and have them monitor our network for any intrusion detection, and geotagging, and that's our use case – to use it to protect our company..”

Verified user

AVP of Tech at a insurance company with 201-500 employees

[Read full review](#) 

“For anyone with an IT footprint in today's cybersecurity-aware landscape, considering solutions like Arctic Wolf (MDR is vital. It is not just for giants like banks; it is particularly valuable for smaller and mid-sized businesses without a dedicated cybersecurity team. When your IT environment surpasses about 50 users, that is when the real need for MDR arises. At that point, you start generating substantial security data, and MDR allows you to tap into expert skills to protect your organization effectively..”

Jared Kruger

Buisness Developer Manager / Sales Executive at Troye

[Read full review](#) 

“One of the things it excels at is flagging vulnerabilities. It scans assets, evaluates the vulnerabilities, and assesses risk scores, focusing on high-risk areas.

It helps to maintain compliance within thirty, sixty, and ninety days as well as, informs us when an asset is out of compliance and the number of days it has been out of compliance. We have agents installed that constantly report back to us from all our data centers. For instance, Log4j and the IBM vulnerability are some issues we've been able to quickly mitigate. .”

Kimberly Brock

[Read full review](#) 

Technical Security Engineer & Data Governance at a computer software company with 51-200 employees

“In my company, we have our own internal MDR as well. I am a salesperson, so I don't use the tool by myself.

I moved from telecom to IT earlier this year. I am very new to the tool, but it sounds great. For our company's clients, the tool increases visibility over the network. Arctic Wolf Managed Detection and Response plugs well into everything. Being able to have that sort of real-time, twenty-four-by-seven help desk that watches over your network and all your devices in case there is some attack or breach that it can contain is helpful..”

Daniele Brommer

[Read full review](#) 

Commercial Manager at Network Service Providers Limited

“We use ArcticWolf as our security operations center (SOC) and managed detect and response (MDR) provider. The primary use case for us was to augment our existing team with additional resources. We did not have the tools or skillsets available, and outsourcing to someone who does makes the most sense.

Our current environment consists of offices/staff around the globe, a few servers, lots of cloud applications, and devices always on the move. We rely heavily on Office 365 and various communication tools to keep our staff connected..”

Verified user

[Read full review](#) 

CIO at Professional Services Organization in Washington DC Area

“We partnered with Arctic Wolf to provide us with 24/7 monitoring of our mixed environment organization.

Arctic Wolf provides coverage for our cloud servers and services, and remote workforce endpoints.

As a relatively small organization with a lean IT staff, we do not have the bandwidth to dedicate ourselves to security 24/7. While our team is security aware, it is not the daily responsibility of any of our team members. We realized we needed a partner that could provide SOC services for our wide-ranging data sources..”

Verified user

[Read full review](#) 

Director of IT Operations at Planalytics, Inc.

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.

“It took us about three to four weeks to bring it live as we had to ship the sensors to different sites. It probably took a month to be fully up to speed, but that was fine because we needed to onboard it anyway..”

Adrian Cambridge

Head of IT at AHMM

[Read full review](#) 

“The initial setup is pretty straightforward. The documentation is pretty good. I rate the ease of setup an eight out of ten. It is a SaaS solution. Two network engineers can deploy the product. We have network engineers and analysts on our team. We make sure the agents are not degraded. Most of the maintenance is done by the vendor..”

Verified user

Service Security Analyst at a government with 11-50 employees

[Read full review](#) 

“The initial setup was somewhat complex, once you set up your scanners and deploy the agents, there is mostly like additional configuration required. Labeling assets and identifying whether they are in production, test, or development is necessary, along with manual inputs. During onboarding, asset labeling tagging is crucial to avoid unknowns. We collaborated extensively with Arctic Wolf on configurations, many of which are integrated into recent product releases and updates to their dashboard. In the beginning we had ongoing meetings with the concierge team until we moved to a more scheduled cadence..”

Kimberly Brock

[Read full review](#) 

Technical Security Engineer & Data Governance at a computer software company with 51-200 employees

“I rate the tool's deployment an eight out of ten, which took nine weeks to complete with two resources. Operational maintenance is relatively minimal and very easy to manage. However, functional maintenance requires a skilled resource like me. The extent of personnel needed depends on the size of the organization. As the organization is not very large, I can handle it independently in my current role. However, I anticipate needing at least five or six people for maintenance tasks in a larger company, such as my previous role. The resource requirement aligns with the company's size..”

Verified user

[Read full review](#) 

security lead at a legal firm with 201-500 employees

“The initial setup was very straightforward.

They provided us with a seamless onboarding experience, and their team guided us through the process of setting up both cloud and on-premise equipment.

They ensured that we had everything set up correctly and even conducted tests to confirm its efficacy.

Their onboarding team did an excellent job of helping us move the project forward from its initial stages to where we are now in our security journey..”

Todd Lienke


[Read full review](#) 

Vice President of Technology at Hallmark Building Supplies, Inc.

“In terms of the initial setup, our involvement is limited as Octopus Deploy handles it directly with the client for compliance and confidentiality reasons. However, the feedback we have received about the setup process has been remarkably positive. It is described as a quick and relatively painless process, typically taking around 30 to 40 days. Even for clients in South Africa, the shipment of sensors and equipment arrives within a month, which speaks to the efficiency of the setup. The choice between cloud or on-premises deployment depends on the client's preference. The solution offers virtual and on-premises sensor deployment options. The setup process is streamlined, with an off-site team collaborating with the client's team. The Security Operations Center is in Germany and works closely with clients for efficient implementation. Clients often install the sensors themselves, and the process is straightforward, making implementation easy..”

Jared Kruger

Business Developer Manager / Sales Executive at Troye

[Read full review](#) 

Customer Service and Support

“They are quite responsive overall. We have monthly meetings where they help us with network security. However, their response can be slow when we ask for more information..”

Adrian Cambridge

Head of IT at AHMM

[Read full review](#) 

“Customer support and service are basically what you are paying for. The technical pieces of the solution are great, however, the ticket response and the quarterly reviews are where the real value is. .”

Verified user

Director, IT Systems and Security at Union Mutual Fire Insurance Company

[Read full review](#) 

“Technical support has been excellent. We haven't had a customer service issue; I have had a few tickets to ask questions, and they have been all handled with high urgency, even if they are not..”

Patti Henderson

IT Director at a legal firm with 51-200 employees

[Read full review](#) 

“Their support is good. If you have questions, you can call them or submit a ticket. They're good to work with. They phoned us about the Exchange vulnerability to walk us through that..”

Verified user

[Read full review](#) 

Senior IT Analyst at a insurance company with 51-200 employees

“I think the technical support for the solution is pretty good. I think it is all about setting expectations with your customers. Arctic Wolf is a global company, so you have to make sure that the customer knows that support will take as per whatever is mentioned in the SLA, which can take three days or whatever. I haven't heard any complaints from my customers about the tool's support team, but nobody is perfect. I rate the technical support an eight out of ten..”

Daniele Brommer

[Read full review](#) 

Commerical Manager at Network Service Providers Limited

“Our experience with technical support from Arctic Wolf is mostly handled by the Octopus technical team, who manage support as the reseller. As a result, our role in providing technical support is limited. The concierge security team, a part of the managed detection and response solution, actively engages with clients to offer technical support, identify vulnerabilities, and conduct proactive threat hunting. This means we are less involved in the technical support aspects of the solution. I would rate Arctic Wolf's technical support as a nine out of ten. Their 24/7 availability of highly skilled security engineers who are responsive to phone calls and emails is a significant strength, with room for minor improvements but very effective overall..”

Jared Kruger

Buisness Developer Manager / Sales Executive at Troye

[Read full review](#) 

Other Advice

“I will recommend the solution to others. It provides more visibility into the environment. If the staff is pretty short-handed, it helps out. Overall, I rate the product a nine out of ten..”

Verified user

Service Security Analyst at a government with 11-50 employees

[Read full review](#) 

“Given the absence of complaints from our customers regarding the solution, I would rate Arctic Wolf MDR very highly, perhaps a ten out of ten. It seems to meet our clients' needs effectively..”

Jared Kruger

Business Developer Manager / Sales Executive at Troye

[Read full review](#) 

“I highly recommend Arctic Wolf as they excel in ensuring the company is well-trained and updated on industry developments.

Overall, I rate them nine out of ten. Their security threat intelligence and timely security bulletins are excellent. They effectively promote a security-conscious culture, raising the bar for security and threat intelligence..”

Kimberly Brock

Technical Security Engineer & Data Governance at a computer software company with 51-200 employees

[Read full review](#) 

“Arctic Wolf is a partner of ours.

I highly recommend Arctic Wolf if you are searching for a partner to assist you in securing your network and if your company is not large enough to afford a full-time CISO on its own.

I would rate Arctic Wolf Managed Detection and Response a nine out of ten..”

Todd Lienke

Vice President of Technology at Hallmark Building Supplies, Inc.

[Read full review](#) 

“Before choosing a security solution, it's crucial to conduct thorough due diligence. Consider factors such as the vendor's approach, strategy, and compliance with data protection regulations like GDPR. Assess the vendor's data centers, their capabilities for shifting data around in case of issues, and their approach to DLP (Data Loss Prevention) detection. Evaluate whether the services offered align with your company's strategy and needs.

Review the different agreements provided by the vendor, including Managed Detection and Response, vulnerability management, and incident response features. Check if your existing cyber insurance can be utilized to cover expenses in case of a breach. Consider whether your organization requires services like vulnerability management and incident response, and choose accordingly.

I rate the product a ten out of ten. .”

Verified user

security lead at a legal firm with 201-500 employees

[Read full review](#) 

“Speaking about the product's integration capabilities, I feel that I am probably not experienced enough to talk about it. Arctic Wolf Managed Detection and Response is still quite immature compared to other providers in the market. The tool sort of integrates with a few products, but it doesn't integrate with everything.

The AI-driven tool helps improve detection and response capabilities, but human beings also manage it. You need the best of both worlds because AI can't do everything. One can still get false positives with the tool, so you need a human being. You also need AI to protect yourself against attacks.

I probably haven't had enough experience to give a proper opinion, but with my experience this year, I think it is pretty good for its current market. It plays in both corporate and medium-sized companies and corporate-level businesses. The tool is not meant for an enterprise-sized business since there are other tools like CrowdStrike and Splunk, along with more mature solutions.

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

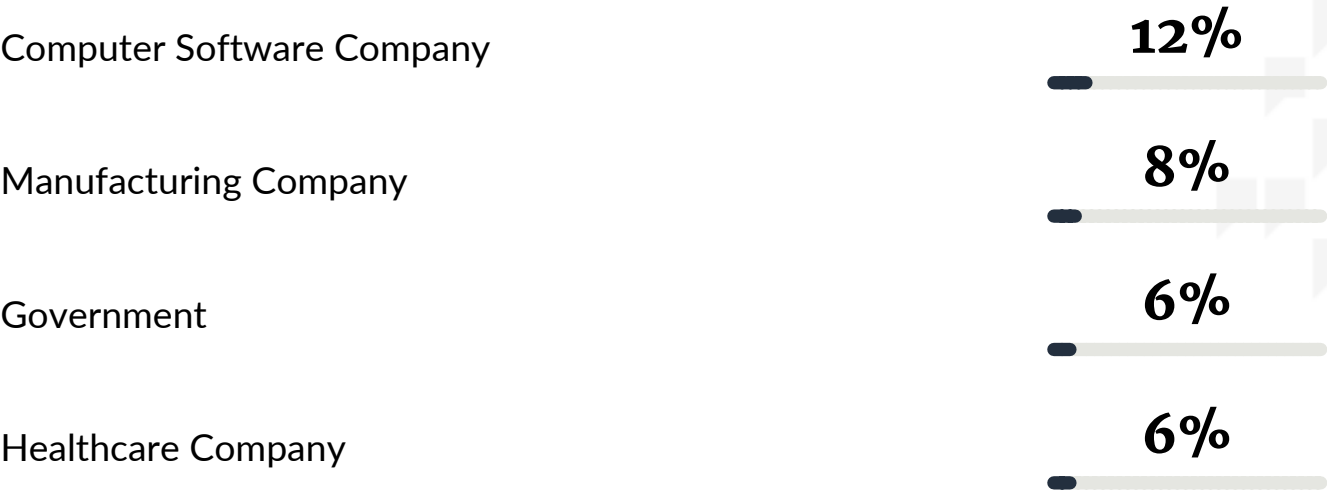
Daniele Brommer

Commerical Manager at Network Service Providers Limited

[Read full review](#) 

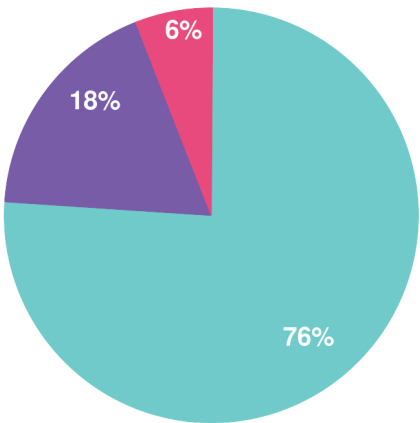
Top Industries

by visitors reading reviews

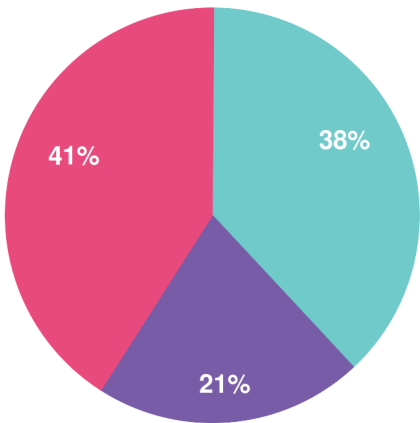


Company Size

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 software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944