aws marketplace

Cyber Security Cloud Managed Rules

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Cyber Security Cloud Managed Rules

Cyber Security Cloud Managed Rules Recap

Cyber Security Cloud Managed Rules enhance web application security by providing features such as automation and real-time updates that minimize manual management and accelerate threat detection.

Cyber Security Cloud Managed Rules deliver an advanced cybersecurity framework for safeguarding web apps and APIs against threats like SQL Injection and DDoS attacks. The rules are seamlessly integrated with AWS WAF and API Gateway, backed by OWASP security, for comprehensive protection. They include automated, real-time updates reducing manual intervention and supporting a security-first approach. Users report enhanced security with fewer successful exploitation attempts due to a decrease in false positives and centralized logging integration. However, the need for enhanced customization and integration with on-prem systems is highlighted by users. The dry run capability and threat intelligence features cater to evolving cyber threats.

What are the key features?

- Free Managed Rules: Stops SQL Injection and Bitcoin mining attacks.
- Bot Control: Manages and mitigates bot traffic effectively.
- Real-time Threat Intelligence: Provides current insights into potential threats.
- Automated Updates: Delivers ongoing, real-time rule updates to minimize manual input.
- Integration Capabilities: Works with centralized logging and XDR SIEM platforms for enhanced security operations.
- Dry Run Capability: Allows safe testing of configurations without disruption.

What benefits should users look for?

- Improved Security: Reduced attack surfaces and fewer exploitation attempts.
- Increased Efficiency: Lesser need for manual management saves time and resources.
- Enhanced Threat Detection: Faster identification and response to threats.
- Customizability: Flexibility in configuring rules to better fit specific security needs.

Cyber Security Cloud Managed Rules are widely used across industries to ensure the safety of e-commerce sites, front-end platforms, and GenAI applications from various cyber threats. Organizations utilize features like rate limiting and telemetry generation for granular insights into attack patterns, enhancing their layered defense strategies and ensuring robust protection against vulnerabilities.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

"The detailed logs and analytics from Cyber Security Cloud Managed Rules help when it comes to making informed security decisions, and it totally depends on the decisions and what logs are needed."

AmitRathod

Senior Analyst at Toll Holdings Limited

"Cyber Security Cloud Managed Rules has positively impacted my organization because earlier, a complete SOC team was required 24/7 for manually checking the alerts, acting upon those alerts, and doing forensics, and with cloud managed rules being automated and intelligent and updating in real time, the manual intervention by the SOC team has been significantly reduced, resulting in a comparatively higher detection rate than before."

Bimal Soun

Network Security Technical Specialist at Wipro Limited

"From my experience, this product is the most stable option available."

Sasikiran Sakalabattina

Sr Infrastructure engineer at TechMahindra

"Cyber Security Cloud Managed Rules has positively impacted our organization because we are a tech company, so we always prefer to get security first."

Lokesh Arora

Senior Software Engineer at Checkout.com

"Cyber Security Cloud Managed Rules has positively impacted my organization; the impact was great."

Dmittal Mittal

Software Engineer at a tech services company with 1-10 employees

"Cyber Security Cloud Managed Rules has positively impacted my organization by reducing the manual WAF management by fifty percent and accelerating the automated updates and improvement in threat intelligence."

Rohit Racharla

Cloud DevOps Engineer at a tech vendor with 10,001+ employees

"Cyber Security Cloud Managed Rules has positively impacted my organization as we have been using it for two years, saving us considerable time because we do not need people to validate traffic or perform any manual deployment anymore."

Verified user

Cloud security engineer at a tech vendor with 10,001+ employees

What users had to say about valuable features:

"The best feature of Cyber Security Cloud Managed Rules is the combination of two capabilities that I appreciate most. The first is automated threat intelligence and rule updates. This solution automatically updates the security signatures to protect against the latest cyber threats, including OWASP attacks, bots, and vulnerabilities without requiring any heavy manual interventions. Automated threat intelligence significantly reduces the operational workload for security teams and improves the overall response time against emerging threats. It also helps organizations maintain stronger security compliance.

The second feature I appreciate most is strong AWS, WAF, and API protection, which is a major strength of Cyber Security Cloud Managed Rules. The seamless integration with AWS and WAF in front of the ALB and API gateway environments provides strong protection against SQL injection or cross-site scripting. In cases of malicious bots and API-based attacks, this solution is highly beneficial for cloud-native and API-driven applications that require scalable and real-time protection.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

"Cyber Security Cloud Managed Rules offers many important features, including confidentiality, which ensures information is only accessed by authorized people. It provides integrity by preventing unauthorized alteration or destruction of data, and availability by ensuring systems and information are available when needed.

"Authentication verifies users, and authorization controls what each user is allowed to access since not everyone has access to all information. Non-repudiation ensures actions or transactions can be traced to the person who performed them, which helps protect information. Threat detection identifies suspicious activities and attacks early to prevent further data loss. Incident response enables quick action to contain cyber attacks. Recovery involves restoring information after data loss occurs, as demonstrated in the hospital example where we quickly intervened to restore their information.

"User awareness training helps staff recognize phishing scams and other threats. These features can be summarized as the CIA triad: confidentiality, integrity, and availability. I also learned that cybersecurity requires continuous monitoring and regular software updates, along with strong passwords, multi-factor authentication, and educating users about cyber threats. Prevention is better than attempting recovery, which is key to keeping systems secure.."

Verified user
CYBERSECURITY PROFESSIONAL /eJPT

Read full review

"The best features Cyber Security Cloud Managed Rules offers include tracking the IPs or bots sending requests that try to attack our servers. I can also block them using these WAF rules, Web Application Firewall rules, which is a good feature.

It is very easy for me to track those IPs and bots using the managed rules, and it integrates well with my dashboards and logs.

Regarding valuable features, the ability to see the IP and the country where the request comes from is very useful when I want to find which countries are getting the most malicious requests and which bots are sending malicious requests. This allows me to block them or add them into my blocked IP list.

Cyber Security Cloud Managed Rules has positively impacted my organization; the impact was great. Since I can track all these malicious requests, I was able to block those, and we do not get attacked much lately since I have been using a Web Application Firewall. I also use their bot rules, where it automatically blocks specific bots which are flagged or blacklisted, which really helps.

I did notice changes in the number of incidents, downtime, and time saved for my team since I started using Cyber Security Cloud Managed Rules. We do not get downtimes now since we have been using this, and the impact is quite positive. Everyone should at least use the basic common rule set of these WAF rules.."

Dmittal Mittal
Software Engineer at a tech services company with 1-10 employees

Read full review

"The best features Cyber Security Cloud Managed Rules offers is that we do not need any manual validation. When it comes to managed rules, it is always tested in my organization and always trusted and authorized in my current infrastructure.

"Automatic validation occurs in my organization because we do not need any manual review in my infrastructure. Whenever there is an issue or a particular application we onboard on our web application firewall, we do not need any manual testing when these managed rules are placed as a major role. Whatever rules we apply, the monitoring is always in good health status with good user agents, and we are always getting traffic from reliable sources. We do not need any manual validation on each and every traffic.

"Cyber Security Cloud Managed Rules has positively impacted my organization as we have been using it for two years. It has saved us considerable time. We do not need people at that particular time to validate those things. It has been a time-saving solution and we do not need any manual deployment anymore.

"Since implementing these managed rules, we have saved time and resources. We have three members working on that, and after implementing Cyber Security Cloud Managed Rules, we have already freed up one more resource from my team. We are now working with two members.."

Verified user

Cloud security engineer at a tech vendor with 10,001+ employees

Read full review

"The best features of Cyber Security Cloud Managed Rules are that there are managed rules available for free that I can implement. I can stop SQL injection attacks, which is one significant vulnerable attack that can be stopped by WAF. Bitcoin mining attacks can also be stopped by implementing WAF. Additionally, there are specific rules related to bot control, which are especially helpful when a bot attacks my website. I implemented a framework known as OWASP Top 10, so these ten security critical vulnerabilities can be mitigated by implementing them.

I implemented free managed rules by AWS, which include Cyber Security Cloud Managed Rules. These managed rules control SQL injection attacks and other attacks that are managed by WAF to prevent them from affecting my systems.

Cyber Security Cloud Managed Rules have impacted my organization very positively because my company is security-focused. We are focusing mainly on security-based setups and implementing everything that can enhance security. This is one of the key applications or services I can implement in my company to stop mitigation attacks, which is why I implemented WAF and attached it to CloudFront, API Gateway, and sometimes to a load balancer to stop and mitigate these attacks.

I noticed specific outcomes or metrics from Cyber Security Cloud Managed Rules in the form of reduced attacks. I discovered that there was no system through which I could conclusively determine what happened, but I noticed some IPs in the logs that were attacking my website and trying to exploit Bitcoin through our platform. This activity was reduced by implementing WAF, and this is what I verified from the logs, which were very helpful.."

Verified user

DevOps Engineer at a tech services company with 11-50 employees

Read full review

“The best features of Cyber Security Cloud Managed Rules include core features that extend protection specific to CMS platforms such as WordPress and Joomla or framework exploits. These rules are regularly updated against the latest CVEs, botnets, and malware without requiring human intervention. I can specify the range in the system and it will update against the latest botnets or malware without requiring any human intervention. It also includes a specialized rule set which mitigates threats targeting web applications, APIs, and serverless environments.

“Cyber Security Cloud Managed Rules help in managing vulnerabilities such as SQL injections and XSS by modeling user and device behavior across the entire cloud estate. If an admin suddenly logs in from a suspicious location or a script makes unusual API calls, Cyber Security Cloud Managed Rules instantly isolates the resource or flags it for review. When a particular threat is recognized, Cyber Security Cloud Managed Rules bypasses the need for human intervention to execute defensive actions such as changing firewall modes, blocking malicious IP addresses, or revoking compromised credentials. I have CI/CD deployment pipelines which are assigned strict scoping to IAM roles, so these roles have the precise permissions required to push updates to Cyber Security Cloud Managed Rules via infrastructure as code. This ensures that every deployment is pre-validated and consistent with the organization's security policies.

“I assess the impact of continuous updates provided by threat intelligence as significant because I have set a particular number of alerts. Whenever I see that this alert is triggered, I conduct monitoring. Based on the manage rules defined in AWS and whatever protocol enforcement exists, my model detects and blocks unauthorized access which deviates from standard HTTPS or other standard protocols, and it mitigates sophisticated bot and malware attacks. API gateway or serverless stage is specifically tuned to block API security and serverless threats. These rules can be natively deployed in front of CloudFront or application load balancer and API gateway. For enhanced operational control, these managed rules are commonly paired with WAF-Champ or automated WAF operation service which helps to manage exception and false positive rates.

“The detailed logs and analytics from Cyber Security Cloud Managed Rules help

when it comes to making informed security decisions, and it totally depends on the decisions and what logs are needed. As long as I have defined all logs related to sign-in logs and audit logs, based on the logs, I decide whether to go with those alerts or whether to minimize that security risk and where to focus.."

AmitRathod
Senior Analyst at Toll Holdings Limited

Read full review

Other Solutions Considered

"I previously used an on-prem solution where everything was done manually, which was expensive regarding employee count and time, with higher chances of error. This prompted us to switch to a hybrid environment that includes both on-prem and cloud solutions.."

Bimal Soun
Network Security Technical Specialist at Wipro Limited

Read full review

"Before deciding on Cyber Security Cloud Managed Rules, we went straight to using these rules. Everything is deployed on AWS, and we want to use AWS. This is the only sole provider for our company, so we are bound to use it.."

Verified user
DevOps Engineer at a tech services company with 11-50 employees

Read full review

"Before choosing Cyber Security Cloud Managed Rules, we did not evaluate other options, though we had some plans to move to Akamai. However, we are satisfied with our current application.."

Verified user
Cloud security engineer at a tech vendor with 10,001+ employees

Read full review

"I have not evaluated other options before choosing Cyber Security Cloud Managed Rules because I first tried AWS Web Application Firewall since my whole project infrastructure was on AWS, which is why I chose AWS Web Application Firewall.."

Dmittal Mittal
Software Engineer at a tech services company with 1-10 employees

Read full review

"Before choosing Cyber Security Cloud Managed Rules, I evaluated other options including on-prem systems and building our servers for automation with tools such as Ansible. I found that the cloud managed rules were easier to set up and better suited for our environment.."

Bimal Soun
Network Security Technical Specialist at Wipro Limited

Read full review

I have not used any other solution before Cyber Security Cloud Managed Rules other than WAF and WAF rules. It has always been that.

Before choosing Cyber Security Cloud Managed Rules, I have always used WAF as a web application firewall and at the network level, we have a network firewall. That is how it has been. At the API Gateway level also we have WAF and even if we expose it via a load balancer, we use WAF. No matter how we expose to the internet, it has always been WAF in the forefront. WAF rules are the thing we have always used. .”

Lokesh Arora
Senior Software Engineer at Checkout.com

Read full review

ROI

Real user quotes about their ROI:

I have seen a return on investment; it has saved money from hackers who demand bounties for application breaches. Regarding time, it is directly taken from the AWS Marketplace, meaning not much time is needed for configuration.

Rohit Racharla Read full review
Cloud DevOps Engineer at a tech vendor with 10,001+ employees

"I have seen a return on investment as we have experienced significant time-saving, which is very good for us. Regarding money saved or return, we have a separate team for that and I am not involved in those calculations.."

Verified user Read full review
Cloud security engineer at a tech vendor with 10,001+ employees

"The return on investment is great. Earlier, we had to manage the whole infrastructure on-prem with a different team at every step, which incurs high costs. With cloud infrastructure, we avoid a significant upfront investment, so it operates on a pay-as-we-grow model, which is beneficial.."

Bimal Soun
Network Security Technical Specialist at Wipro Limited

Read full review

"I have seen a return on investment with Cyber Security Cloud Managed Rules. It really saved my time debugging attacks by showing me where the attack came from, whether it was detected, and how to prevent it. Since I have been using WAF, these incidents are very less frequent than before. It is really helpful for the person in charge of security for the cloud infrastructure.."

Dmittal Mittal
Software Engineer at a tech services company with 1-10 employees

Read full review

I would say time saved is a big metric as a return on investment with Cyber Security Cloud Managed Rules because we are not always looking for things manually or stopping attacks manually. This is helpful because we have automated WAF rules, so they obviously come to the forefront and help protect us against any of the attacks. That is a time save. We have alerts configured if there is an issue. We do not have to manually go and find out about those issues; we usually get an idea of what is going on. A big benefit would be time save, which in engineering can be converted to money saved as well.

Lokesh Arora
Senior Software Engineer at Checkout.com

Read full review

Use Case

"Cyber Security Cloud Managed Rules protects digital systems, networks, devices, applications, and data from unauthorized access. The key purposes include data protection by preventing theft and leakage of sensitive information, and preventing cyber attacks such as malware, ransomware, phishing, and hacking.."

Verified user
CYBERSECURITY PROFESSIONAL /eJPT

Read full review

"In day-to-day security operations, I primarily focus on protecting web applications, APIs, and cloud workloads. From my experience, this product is the most stable option available. It significantly manages applications during cyber-attacks and addresses threats in AWS environments, including traffic patterns from malicious bots and SQL injections. The product is very helpful for managing these scenarios.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

"My main use case for Cyber Security Cloud Managed Rules is to protect from malware like DDoS incidents, against cross-site scripting, against SQL injections, and against geofencing. These are the areas which we majorly use cloud security and our cybersecurity managed rules.

"A recent scenario of how I use Cyber Security Cloud Managed Rules to protect against one of those threats is that we have a specific application where only Italy is in-market, which means only Italian people can access that site because our sales are only in the Italian market. However, when we get human traffic from countries like Nigeria, Iran, and Pakistan, where we do not have any sales, the traffic still comes from such countries as DDoS requests. Cyber Security Cloud Managed Rules automatically blocks those countries where we do not have sales.."

Verified user

Cloud security engineer at a tech vendor with 10,001+ employees

Read full review

"My main use case for Cyber Security Cloud Managed Rules is to protect against malicious attacks like SQL injection attacks and cyber attacks.

Recently, I discovered malicious IPs which I believed were operating as a botnet and attacking my e-commerce website. Because WAF is for web application security, I used WAF managed rules related to IP and IP injection attacks. There are additional rules available for IP rate limiting based attacks, which allow me to implement a maximum number of attempts from a particular IP within a specific time period. This rate-limiting rule helps prevent unknown IPs from accessing my website.

The general security vulnerabilities provided by AWS WAF through managed rules or custom rules that I can implement will protect my application and enhance the security of my application through these security rules. This is the main use case of implementing WAF rules.."

Verified user

DevOps Engineer at a tech services company with 11-50 employees

Read full review

"My main use case for Cyber Security Cloud Managed Rules is to prevent basic cyber attacks that happen most commonly using a Web Application Firewall.

Regarding my main use case and experience, the Web Application Firewall handles basic attacks. There is also a dashboard where I can check how these rules are blocking requests. I can check from which countries are sending more vulnerable requests towards us, which is very useful.

I can give a specific example of a situation where I used the managed rules to block or prevent an attack. In my recent project, the Web Application Firewall prevented attacks such as SQL injection, cross-site scripting, and brute force attempts. I was getting many requests from different servers, which may have been a DDoS attack. I had already written a managed rule for this situation. I created a custom rule in which if many requests come from a specific source, they will be blocked.."

Dmittal Mittal
Software Engineer at a tech services company with 1-10 employees

Read full review

"I work in the IAM domain, and we combine Cyber Security Cloud Managed Rules with IAM, which allows us to enforce least privilege security posture and automate response to cyber threats. Cyber Security Cloud Managed Rules relate to IAM controls who can access cloud resources, while Cyber Security Cloud Managed Rules dictate how those resources are protected against network level and application level attacks. They eliminate the need for manual firewall creation by automatically blocking web application vulnerabilities and attacks.

"I occasionally use the real-time monitoring feature of Cyber Security Cloud Managed Rules because we do not have a regular deployment schedule. Whenever we conduct a major change in production deployment, I use this system to track vulnerabilities, API exploits, and any malware activity. This usage is occasional and depends on the deployment in production.."

AmitRathod
Senior Analyst at Toll Holdings Limited

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 experience with pricing, setup cost, and licensing for Cyber Security Cloud Managed Rules is straightforward. I have a dedicated team that takes care of this, and I am not much involved in those activities. I provide them with my requirements, and they provide solutions accordingly.

Rohit Racharla

Read full review

Cloud DevOps Engineer at a tech vendor with 10,001+ employees

"Deploying Cyber Security Cloud Managed Rules is moderate in complexity. I encountered no challenges deploying Cyber Security Cloud Managed Rules. It takes almost two weeks to deploy Cyber Security Cloud Managed Rules.."

AmitRathod

Read full review

Senior Analyst at Toll Holdings Limited

"Initial deployment depends on the environment being used. In my case, we are using two cloud environments, and the initial deployment is not very difficult. My organization is a medium-scale organization already using AWS infrastructure. The setup process is simple because the rules can be directly subscribed and deployed with AWS Marketplace in AWS WAF. Its integration with CloudFront, application load balancer, and API gateways is straightforward and can be completed within a short time. The initial deployment is manageable, and this product also provides predefined management rules, reducing the need for writing custom security policies manually.

After deployment, some tuning and monitoring are required to handle false positives related to application-based traffic behavior, where most organizations initially deploy the rules in count mode before switching to blocking mode to avoid impacting genuine users. Overall, compared to traditional WAF deployments, Cyber Security Cloud Managed Rules is easier, faster, and requires less operational effort for implementation.."

Sasikiran Sakalabattina

Sr Infrastructure engineer at TechMahindra

Read full review

Customer Service and Support

"The customer support for Cyber Security Cloud Managed Rules is excellent. Whenever we raise a request, whether it is high critical or small to medium critical cases, the customer support responds quickly. Within just a few minutes, we receive a response from them.."

Verified user
Cloud security engineer at a tech vendor with 10,001+ employees

Read full review

"I would describe the customer support for Cyber Security Cloud Managed Rules as pretty average. They provide a link and then disappear, so I have to do my own research. My experience with support was not good.."

Dmittal Mittal
Software Engineer at a tech services company with 1-10 employees

Read full review

"Customer support for Cyber Security Cloud Managed Rules is great, as it is easy to reach out compared to on-prem vendors, and overall, I am satisfied with the customer support provided.."

Bimal Soun
Network Security Technical Specialist at Wipro Limited

Read full review

The customer support for Cyber Security Cloud Managed Rules is generally good. It depends on the vendor, which is AWS when it comes to AWS WAF and Fastly when it comes to Fastly customer support.

Lokesh Arora
Senior Software Engineer at Checkout.com

Read full review

"I engage with the technical support team regularly. The support team helps with rule tuning, false positive handling, deployment guidance, and troubleshooting during security incidents. Sometimes we are unable to handle incidents from a security perspective, and even though false alerts regularly occur, we engage with vendor support. For any issues, we need to raise a ticket via the vendor portal. Initially, we write an email, and after the ticket is created, they check the issue and arrange a call. For standard operational issues, the response time is acceptable, and the support documentation is useful. During critical incidents, for complex applications or specific issues, the response is faster, and troubleshooting support is required. Overall, the technical team is knowledgeable about this product and assists effectively in maintaining stable day-to-day operations.."

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

Other Advice

"I would advise others looking into Cyber Security Cloud Managed Rules to use WAF if they want to eliminate security attacks, especially if they are using AWS. I would rate this product 8 out of 10.."

Verified user
DevOps Engineer at a tech services company with 11-50 employees

Read full review

"Human error is one of the biggest security risks. Simple actions such as clicking a suspicious link or using a weak password can expose sensitive information. Cybersecurity is not only about protecting computers; it also involves protecting data, people, networks, and organizations from cyber threats.."

Verified user
CYBERSECURITY PROFESSIONAL /eJPT

Read full review

"Everyone should use these rules for better security for their applications and implement them. Additionally, they should learn from the mistakes they make when implementing rules for the future. I give Cyber Security Cloud Managed Rules an overall rating of eight out of ten.."

Dmittal Mittal
Software Engineer at a tech services company with 1-10 employees

Read full review

"I would rate Cyber Security Cloud Managed Rules around nine out of ten. I chose nine out of ten because even if it is perfect, I would not give a ten because there is no world called perfection in this world. We are humans, and maximum nine is sufficient for each and every field. I would not rate anything ten out of ten. I would advise others looking into using Cyber Security Cloud Managed Rules to go for this because the world is changing in technology, and for security, there should be no compromise. I always recommend them and advise them to go for Cyber Security Cloud Managed Rules. My overall review rating for this product is nine out of ten.."

Verified user
Cloud security engineer at a tech vendor with 10,001+ employees

Read full review

“Maintaining rules is relatively low compared to traditional WAF because most security rules and threat signatures are automatically updated by the vendor. The day-to-day activities mainly include monitoring alerts, checking the server's behavior, checking disk alerts, and reviewing blocked requests while handling false positives. Regular log analysis and policy reviews are still required to ensure smooth operations based on performance and security compliance. Maintenance efforts related to rules are low compared to traditional WAF. This solution also reduces the dependency on manual patching, which usually requires logging into the server for Windows updates. The process is simple, and the product is straightforward to maintain, helping significantly reduce the operational workload through automation and centralized management where everything can be managed from one dashboard. I would rate this solution a nine out of ten overall..”

Sasikiran Sakalabattina
Sr Infrastructure engineer at TechMahindra

Read full review

"When I compare Cyber Security Cloud Managed Rules with FortiNets, I see that FortiNets is used for both on-premises as well as for cloud, but mostly on-premises; FortiNet is mainly focused on on-premises. Cyber Security Cloud Managed Rules is a natively cloud platform that provides website performance and edge security. Most WAF is related to only cloud-based solutions.

"I would advise others looking to implement Cyber Security Cloud Managed Rules that it depends on their requirement. If they want an on-premises solution, then they should go for Fortinet, and if they want a cloud solution, then they should go for WAF Cloudflare.

"I would rate this product overall at a nine out of ten.."

AmitRathod
Senior Analyst at Toll Holdings Limited

Read full review

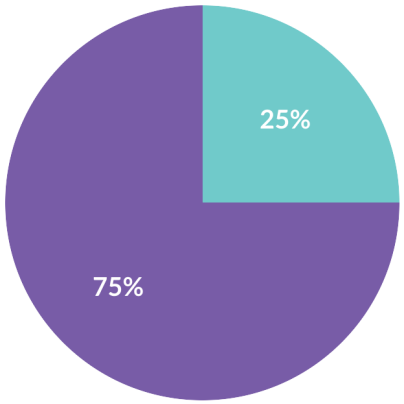
Top Industries

by visitors reading reviews

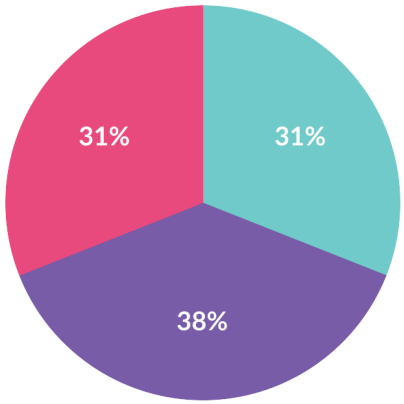
Construction Company	27%
Logistics Company	12%
Outsourcing Company	12%
Comms Service Provider	6%

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