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 are designed to mitigate and minimize vulnerabilities, including all those on OWASP Top 10 Threats list. With the HighSecurity OWASP Set, you can start protecting your web applications right away with a low false-positive rate and a higher defense capability.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "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

- "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 by reducing the manual WAF management by fifty percent and accelerating the automated updates and improvement in threat intelligence."

Rohit Racharla

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

"Cyber Security Cloud Managed Rules have impacted my organization very positively because my company is security-focused."

Verified user

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

What users had to say about valuable features:

The best features that Cyber Security Cloud Managed Rules offers include low false positive rates, bot detection, zero-day threats, real-time authentication, and real-time threat intelligence.

In my day-to-day work, I find the malicious bot detection feature of Cyber Security Cloud Managed Rules to be the most valuable.

"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 Engineer at a tech vendor with 10,001+ employees

Read full review

The best feature that Cyber Security Cloud Managed Rules offers in my experience is the ability to roll it out in a dry run, which would be a useful way of testing things without impacting real user traffic. After implementing the rules, I would need good observability to get an idea of how effective they are and what I should change to make them better.

Cyber Security Cloud Managed Rules has positively impacted our organization because we are a tech company, so we always prefer to get security first. This is a big thing when it comes to exposing any domain. We would want to ensure that we have secure guardrails around it, and whenever we roll it out, we properly ensure that there was a design doc, there was a review, and make sure that it was behind those security gates to avoid any issues after go-live. It is a proper process that we follow to ensure that no new application sneaks through and before go-live, all these checks are done. ."

Lokesh Arora
Senior Software Engineer at Checkout.com

Read full review

"The best features Cyber Security Cloud Managed Rules offers are mainly that there is less human intervention, which reduces the chances of error, and it is also less time-consuming and more intelligent compared to manual rules.

"When I mention more intelligent, Cyber Security Cloud Managed Rules stands out in that these rules are generally updated according to the latest cyber attacks and the latest signatures in the system, so we don't need to manually change the rule, as they get updated mostly in real time, making detection easier.

"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. 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

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

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

Read full review

"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 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

My main use case for Cyber Security Cloud Managed Rules is for the API Gateway and for OWASP security.

I am integrating these WAF rules with the API Gateway and CloudFront to ensure security from cybersecurity issues, minimizing vulnerabilities and mitigating threats from hackers, including the OWASP top 10 web application threat lists. I have configured it for our front end and for the API Gateway.

“I am using Cyber Security Cloud Managed Rules for our GenAI applications, specifically for the chatbot I have recently created, which helps tremendously and prevents hackers' exploits in our application. .”

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

Read full review

"My main use case for Cyber Security Cloud Managed Rules is the protection of any cyber attack on my API servers and cloud managed rules on my WAF.

"A specific example of how I use Cyber Security Cloud Managed Rules to protect my API servers is that we have an AWS WAF at the parameter level where we have implemented the OWASP top 10 attack rule as a cybersecurity managed rule in the parameter. Any traffic coming to our API server passes through the WAF, and the WAF OWASP top 10 rule filters that traffic for any attack.."

Bimal Soun
Network Security Technical Specialist at Wipro Limited

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

Our main use case for Cyber Security Cloud Managed Rules is mostly web application because it protects the front end and also with the CDN we are using it, so it protects the CDN exposed applications as well.

A specific example of how we have used Cyber Security Cloud Managed Rules to protect our web applications or CDN is that we have a proper dashboard of all attacks that were attempted on those exposed URLs at the application level and we have clear visibility. Whenever there is some type of IP which is trying to DDoS our domain, then it gets automatically blocked and we have configured alerts as well. We do get a consolidated report weekly and monthly that shows a lot of hits, what the IP was, and that it was automatically blocked.

“We also have AI workload, so it is important to consider that in our main use case for Cyber Security Cloud Managed Rules. We are catering to that in our workflow and trying to manage it so that even our AI workflows do not have prompt injections or, if we are having agents, we do not get man-in-the-middle attacks with the prompts. .”

Lokesh Arora
Senior Software Engineer at Checkout.com

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

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

Read full review

Customer Service and Support

"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

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

I surely recommend using Cyber Security Cloud Managed Rules for AI applications because, as a cloud engineer and operations engineer, I feel more comfortable using these cybersecurity managed rules without any issues in real-time.

I do not have any additional thoughts about Cyber Security Cloud Managed Rules at the moment, but if I encounter something while developing more agentic AI applications in the future, I hope to find something helpful for improving the cybersecurity managed rules. I have provided this review with a rating of seven. .”

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

Read full review

“My advice to others looking into using Cyber Security Cloud Managed Rules is to maintain a blend of on-prem and cloud solutions, while also performing regular checks and balances on the cloud managed rules to observe their behavior with applications.

“My additional thoughts on Cyber Security Cloud Managed Rules are that the

effectiveness largely depends on the specific business use case, as it will not fit every business logic. Sometimes, there is over-blocking within the cloud managed rules where valid requests or IPs could be blocked, which should be fine-tuned to reduce over-blocking. I would rate this product an 8 overall.."

Bimal Soun
Network Security Technical Specialist at Wipro Limited

Read full review

In terms of how I use dry run mode and observability with the managed rules, we implement it in a count mode. We will only not block any traffic, but just get a count and get an idea of how the rule would work. Observability-wise, generally in Fastly CDN, we do get a dashboard of how the traffic is getting served. If there is some kind of suspicious IPs or any IP set which is coming from a certain country which we do not want the traffic coming from, then it gets blocked. We have proper visibility.

I think the AI space is something really big right now, so I would to see some improvements around those lines.

"I am not one hundred percent sure if we purchased Cyber Security Cloud Managed Rules through the AWS Marketplace. We may have, but I have not looked into that.

"I have not been involved in the pricing, setup cost, and licensing phase for Cyber Security Cloud Managed Rules. It usually comes via procurement, so I am not involved in the licensing side of things because I am mostly technical and I am someone who implements things. I have not come across looking at the pricing, licensing, or setup cost.

"I would give Cyber Security Cloud Managed Rules an overall rating of seven. ."

Lokesh Arora
Senior Software Engineer at Checkout.com

Read full review

Top Industries

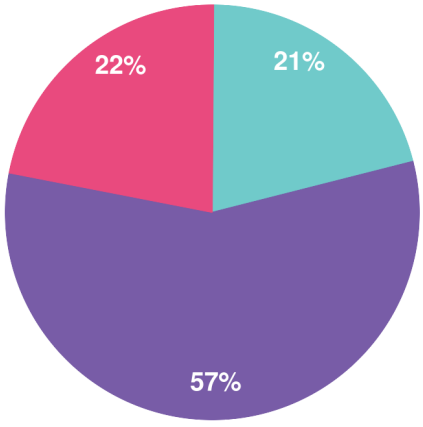
by visitors reading reviews

Construction Company	46%
Comms Service Provider	6%
Energy/Utilities Company	6%
Manufacturing Company	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 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