aws marketplace

Imperva Managed Rules on AWS WAF

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Imperva Managed Rules on AWS WAF

Imperva Managed Rules on AWS WAF Recap

Imperva Managed Rules on AWS WAF offers advanced protection against web application attacks with rule sets designed for efficient threat management.

This solution provides a comprehensive layer of security by integrating seamlessly with AWS infrastructure. Targeting vulnerabilities, it ensures robust protection while minimizing false positives. With easy rule management, users can dynamically address threats, maintaining optimal security postures across AWS environments. This allows for tailored security strategies tailored to specific application requirements.

What are the valuable features?

- Comprehensive Coverage: Protects against OWASP Top 10 threats.
- Auto Updates: Regular rule updates to combat emerging threats.
- Custom Rule Support: Allows creation of user-defined rules.
- Detailed Reporting: Offers insights into security events.
- Seamless Integration: Works easily with AWS infrastructure.

What benefits should users look for in reviews?

- Cost Efficiency: Reduction in manual intervention and faster threat resolution.
- Enhanced Security: Improved protection against sophisticated threats.
- Flexibility: Adaptable to specific application security requirements.
- Reduced False Positives: Accurate threat detection minimizing interruptions.
- Scalability: Aligns with evolving application demands.

In industries like e-commerce and finance, Imperva Managed Rules on AWS WAF is used to safeguard customer data while improving customer trust by efficiently mitigating security threats. These sectors benefit from the customizable and automated threat response capabilities that align with high-demand security standards.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The managed rule set proves that modern security does not have to be slow or complicated."

BasilJiji

System engineer at a retailer with 10,001+ employees

- "Imperva Managed Rules on AWS WAF has positively impacted my organization by addressing trust issues my customer had regarding security configuration for their application."

Indikad IS

Head Of Cloud & Customer Success at a university with 501-1,000 employees

- "Automatic updates are the best features Imperva Managed Rules on AWS WAF offers."

Miguel Ángel Carvajal Ramos

Cloud Engineer at Universidad Nacional Autónoma de México (UNAM)

"Imperva Managed Rules on AWS WAF offers continuous threat intelligence updates as the best feature, as they have a rapid response to newly discovered attack techniques and base their detection logic on real-world threat data with easy integration with AWS."

Ayodeji Bayo-Makinde

Technical Support Engineer at Horizon/Bespoke Labs

"Imperva Managed Rules on AWS WAF has impacted my organization positively to a very good extent, as along with the default AWS WAF rules, Imperva Managed Rules on AWS WAF is giving more edge on layer seven security for protecting the applications at the organization, making them good-to-go rules."

Verified user

Senior Consultant at a tech vendor with 10,001+ employees

What users had to say about valuable features:

"I use Imperva Managed Rules on AWS WAF because they have a rapid response to newly discovered attack techniques, and it is quickly updated, reducing the need for our internal security teams to create custom rules.

"Imperva Managed Rules on AWS WAF offers continuous threat intelligence updates as the best feature, as they have a rapid response to newly discovered attack techniques and base their detection logic on real-world threat data with easy integration with AWS.

"It has greatly reduced operational overhead, because without Imperva Managed Rules on AWS WAF, we would have to dedicate a team to analyze traffic attacks, write custom WAF rules, test the rules, and then maintain signatures. Imperva Managed Rules on AWS WAF helps to handle much of this maintenance work and allows our teams to focus on higher priorities.."

Ayodeji Bayo-Makinde
Technical Support Engineer at Horizon/Bespoke Labs

Read full review

"The best feature I would say is the compliance. It satisfies enterprise audit criteria for web application profiling that is required by PCI DSS and HIPAA. Also, it aligns fully with my security compliance matrices, the OWASP Top 10 alignment, and standard core rules to defend against injection attacks, cross-site scripting, and path traversal. These are the major features.

"The managed rule set proves that modern security does not have to be slow or complicated. It turns threat intelligence into a utility function that I can enable with a few clicks.

"It has eliminated the heavy operational burden of threat research. Instead of my internal security engineers spending hours tracking new malicious IPs or writing custom regex signatures to deal with emerging exploits, Imperva automatically updates the rule set in the background.."

BasilJiji
System engineer at a retailer with 10,001+ employees

Read full review

“In my opinion, the best features Imperva Managed Rules on AWS WAF offers include malicious bot detection and app-specific protections. I have seen that the malicious bot detector was able to identify the changing nature of the attack, helping me manage it from Imperva.

“Imperva Managed Rules on AWS WAF has positively impacted my organization by addressing trust issues my customer had regarding security configuration for their application. My customers expected us to be consultants, and unfortunately, previous products did not have that capability. Imperva's ability to identify the best configuration was amazing.

“Regarding positive outcomes after switching to Imperva Managed Rules on AWS WAF, I have control over security incidents and have seen a decrease in incidents. This helped improve the trustworthiness with the customer, along with improved application reliability and stability. These are the proactive and positive results based on my scenarios with Imperva..”

Indikad IS

Head Of Cloud & Customer Success at a university with 501-1,000 employees

Read full review

“Automatic updates are the best features Imperva Managed Rules on AWS WAF offers. When I mention updates, I am referring to the automatic threat intelligence and frequency of rule updates. Imperva automatically updates threat intelligence and signatures, which saved a lot of engineering teams considerable time.

“The customer support for Imperva Managed Rules on AWS WAF is the best. As soon as I had any issue when I was on-call rotation, the support was very friendly, very accurate, and always helpful.

“Imperva Managed Rules on AWS WAF's governance and security is very robust. The security and compliance is always the best. If you do not have proper roles or privileges, it's impossible to access information or details from other users or accounts.

“Imperva Managed Rules on AWS WAF's accuracy and reliability of output is very accurate. I would say it's one of the industry standards, with more accuracy. I have never seen greater accuracy with Imperva or Incapsula..”

Miguel Ángel Carvajal Ramos
Cloud Engineer at Universidad Nacional Autónoma de México (UNAM)

Read full review

“The best features of Imperva Managed Rules on AWS WAF are that all the rules are in line with the updated OWASP Top 10 security vulnerabilities, which allows me to counter attack with the respective attack patterns that are present in the market.

“Staying up to date with the latest OWASP Top 10 has helped my team significantly, as with the updated 2026 rules, we can counter the cyber attacks that are more aligned with artificial intelligence tools. Earlier, there were certain OWASP Top 10 rules that were not present in the environment.

“Imperva Managed Rules on AWS WAF has impacted my organization positively to a very good extent, as along with the default AWS WAF rules, Imperva Managed Rules on AWS WAF is giving more edge on layer seven security for protecting the applications at the organization, making them good-to-go rules.

“Since using Imperva Managed Rules on AWS WAF, I've noticed specific outcomes such as a reduction in security incidents, and it provides me with more robust solutions along with protections and analysis, allowing it to protect against cyber attacks at any level or capacity..”

Verified user

Senior Consultant at a tech vendor with 10,001+ employees

Read full review

Other Solutions Considered

"I previously managed custom IP blocklists manually via standard network firewall rules. I switched because manual lists are reactive, rigid, and impossible to maintain efficiently against rapidly changing cloud threat vectors.."

BasilJiji
System engineer at a retailer with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

"I have seen a return on investment when something involves any deployment for blue or green deployment. I was in charge of redirection rules, so traffic from one cluster to another was very useful.."

Miguel Ángel Carvajal Ramos
Cloud Engineer at Universidad Nacional Autónoma de México (UNAM)

Read full review

"The return on investment is highly visible in my infrastructure savings. By stopping illegitimate traffic at my utmost edge, I noticed a 15% drop in junk traffic reaching my application layers. This reduced my downstream compute cost and lowered my database resource consumption.."

BasilJiji
System engineer at a retailer with 10,001+ employees

Read full review

Use Case

“My main use case is proactive edge security and IP reputation management. I use Imperva Managed Rules on AWS WAF's IP reputation rule group attached to my main application load balancer. Because Imperva leverages crowd-sourced global threat intelligence from their entire network, the rule layer automatically blocks requests originating from known botnets, exit nodes, and active attackers. For example, during a distributed credential stuffing attempt, Imperva dropped the malicious connections at the AWS edge layer instantly. This saves my back-end applications' API from resource exhaustion..”

BasilJiji
System engineer at a retailer with 10,001+ employees

Read full review

"My main use case for Imperva Managed Rules on AWS WAF is using Layer 7 particular OWASP 10 and SP10 based security rules. I had to enable the Layer 7-based attacks by setting up bots and related configurations, so that was the primary case. On WAF, I set up those rules for the particular finance application security part.

"Imperva Managed Rules on AWS WAF has helped my finance application specifically by allowing us to identify bots and adapt to attacks that were changing over time. Once I identified Imperva's product capability and set up those rules, I was able to rectify the attacks that I was not able to prevent with previous products.."

Indikad IS

Head Of Cloud & Customer Success at a university with 501-1,000 employees

Read full review

"Imperva Managed Rules on AWS WAF was used to protect high traffic enterprise web applications and APIs, handling millions of monthly requests. I was part of the domain management and CDN network team. It served as the primary baseline security layer, integrated directly into AWS web ACLs.

"Imperva Managed Rules on AWS WAF is deployed in a hybrid cloud environment in my organization. We have direct traffic from Akamai CDN, but everything was passing through Imperva.."

Miguel Ángel Carvajal Ramos
Cloud Engineer at Universidad Nacional Autónoma de México (UNAM)

Read full review

“My main use case for Imperva Managed Rules on AWS WAF is to protect my layer seven applications and application load balancers (ALBs) so that I can protect my applications from layer seven cybersecurity attacks.

“I can give a specific example of how I've used Imperva Managed Rules on AWS WAF to protect an application, as the rules help me protect from cyber attacks which are part of the OWASP Top 10, including cross-site scripting, SQL injection attacks, and sometimes modifications of MFA for specific applications.

“I'm mainly focusing on protecting my applications that are hosted on CloudFront and sometimes on the application load balancer in AWS, for which I'm using Imperva Managed Rules on AWS WAF..”

Verified user

Senior Consultant at a tech vendor with 10,001+ employees

Read full review

“I use Imperva Managed Rules on AWS WAF in front of AWS WAF to extend the native capabilities, leveraging Imperva's threat intelligence and web application security expertise to provide pre-configured protections against common web attacks while also helping to reduce operational burden on the team.

“Recently, we worked on creating a payment gateway, and we used Imperva Managed Rules on AWS WAF to help stop threats such as SQL injection, cross-site scripting, command injection, local file inclusion, and path traversal, essentially all OWASP threats.

“You can also use the WAF policy with Application Load Balancers, CloudFront distributions, and API Gateway endpoints on AWS, with most deployments being able to be completed in a few hours.

“Imperva Managed Rules on AWS WAF is a very good tool, but you need to consider your use case, as it is well-suited for healthcare systems, financial applications, organizations with small security teams, those trying to improve compliance, and public-facing web applications exposed to the internet. However, if you have internal-only applications or small websites with minimal risk, and if your organization requires full control over detection rules, Imperva Managed Rules on AWS WAF would not work, and you must be willing to tune the WAF behavior even after deploying Imperva, or it will not work for you..”

Ayodeji Bayo-Makinde
Technical Support Engineer at Horizon/Bespoke Labs

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.

"I fixed this by putting Imperva Managed Rules on AWS WAF's rule group into count mode for the first two weeks. This allowed me to analyze the traffic pattern safely in my logs and write specific bypass exceptions before switching the rules to strict block mode.."

BasilJiji

Read full review

System engineer at a retailer with 10,001+ employees

"When it comes to configuring and managing malicious bot detection and app-specific protections, the configuration was not an issue, although I had to run it on a few cycles. I set it up and it was not the proper configuration in the first phase. In the second phase, I added a few additional configurations with several application attributes that helped me protect the application properly. Fine-tuning the rules required work in a few phases, but overall, the configuration was smooth.."

Indikad IS

Read full review

Head Of Cloud & Customer Success at a university with 501-1,000 employees

"Imperva Managed Rules on AWS WAF was integrated very quickly without having to build custom rule sets from scratch, positively impacting my organization.

"The quick integration of Imperva Managed Rules on AWS WAF benefited my team with compliance like PCI DSS and SOC 2. It was integrated very quickly without creating something from scratch. The security compliance audits were easier.."

Miguel Ángel Carvajal Ramos

Cloud Engineer at Universidad Nacional Autónoma de México (UNAM)

Read full review

Customer Service and Support

"The customer support for Imperva Managed Rules on AWS WAF is quite good; I have used it once and received good responses. For my one experience, I would rate the customer support a nine, as it was good.."

Ayodeji Bayo-Makinde
Technical Support Engineer at Horizon/Bespoke Labs

Read full review

"The customer support is providing excellent service. The support and reference models are very structured. AWS documentation explicitly outlines how to subscribe to and deploy vendor rule sets, while Imperva provides clear definitions for what each rule group evaluates. Support for rule matching is managed through AWS Premium Support channels with escalation lines to Imperva's threat research team for enterprise subscribers.."

BasilJiji
System engineer at a retailer with 10,001+ employees

Read full review

"The customer support for Imperva Managed Rules on AWS WAF is the best. As soon as I had any issue when I was on-call rotation, the support was very friendly, very accurate, and always helpful.

"I would rate the customer support a ten out of ten.."

Miguel Ángel Carvajal Ramos
Cloud Engineer at Universidad Nacional Autónoma de México (UNAM)

Read full review

"I had very few incidents requiring customer support for Imperva Managed Rules on AWS WAF. Before that, I was able to manage most issues myself. Although I don't have extensive experience, the level of support I received during the incidents was very much supportive.

"I would rate customer support as an eight on a scale of one to ten.."

Indikad IS
Head Of Cloud & Customer Success at a university with 501-1,000 employees

Read full review

Other Advice

"I have not really made use of the AI capabilities of Imperva Managed Rules on AWS WAF, but from what I have heard from others, it seems it is quite standard for the market.

"For my end, the cost of Imperva Managed Rules on AWS WAF might sometimes be a bit high, making it not suitable for small websites with minimal risk because the cost outweighs the benefits in that case. However, for a big e-commerce platform or payment gateway, it is definitely a worthwhile investment.

"I can definitely speak to the fewer employees needed because the time and effort it would take to dedicate engineers or resources to create custom WAF rules is cut out by using Imperva Managed Rules on AWS WAF.

"I would rate this solution an eight overall.."

Ayodeji Bayo-Makinde
Technical Support Engineer at Horizon/Bespoke Labs

Read full review

"Imperva Managed Rules on AWS WAF is great for meeting security compliance audits, using the out-of-the-box compliance and low operational overheads.

"I highly recommend Imperva Managed Rules on AWS WAF when you need something fast and low-maintenance threat protection. For applications with highly customized API payloads, there may be some false positives.

"I would highly recommend Imperva Managed Rules on AWS WAF when you need fast, low-maintenance threat protection.

"I would like to continue using Imperva and integrate it with Terraform, so my pipelines will be much more secure.

"I give this review an overall rating of eight out of ten.."

Miguel Ángel Carvajal Ramos
Cloud Engineer at Universidad Nacional Autónoma de México (UNAM)

Read full review

“Everything looks good with Imperva Managed Rules on AWS WAF as of now.

“Regarding Imperva Managed Rules on AWS WAF's AI capabilities, I believe it has a good alignment from the governance and security perspective, and it is capable of protecting from cyber attacks effectively.

“In terms of accuracy and reliability of output regarding Imperva Managed Rules on AWS WAF's AI capabilities, it all depends on which AI generative model is being used. Currently, Imperva is in good shape with a decent capacity for accuracy and reliability, though not perfect.

“My advice to others looking into using Imperva Managed Rules on AWS WAF is that if customers do not want to use the default AWS WAF rules or if they are looking for add-on features or protection, they should proceed with Imperva Managed Rules on AWS WAF to gain more security.

“I give this product a rating of 9 out of 10..”

Verified user
Senior Consultant at a tech vendor with 10,001+ employees

Read full review

“I wanted to add timestamps of bot-based activity, as I don't want unwanted latency for my applications, but I also require security. If I could configure timestamp-based rules to identify the particular configuration, that would be a better approach.

“I rate Imperva Managed Rules on AWS WAF a seven on a scale of one to ten, as I believe there is room for improvement. When comparing it to the previous WAF product, Fortinet, I would give Fortinet around three marks.

“I chose seven specifically due to my experience managing applications and the high standard of behavior management from Imperva, particularly in managing the behavioral changes of Layer 7 attacks through malicious bot protection, which

is the key reason for my rating of seven.

“My advice for others looking into using Imperva Managed Rules on AWS WAF is to focus on security since application security is critical. I cannot compare the product cost with others because a single incident can result in significant losses. Choosing the best product with the capability of protecting your application is essential. Imperva with AWS WAF configuration enables a high level of global availability of WAF settings that help manage many security challenges.

“Before concluding, I would say there should be a focus on the governance aspect of Imperva Managed Rules on AWS WAF, as applications have many integrations with other systems. Compromising another application could challenge my application, so managing other integrations effectively in governance would be beneficial. My overall rating for Imperva Managed Rules on AWS WAF is seven out of ten..”

Indikad IS
Head Of Cloud & Customer Success at a university with 501-1,000 employees

Read full review

Top Industries

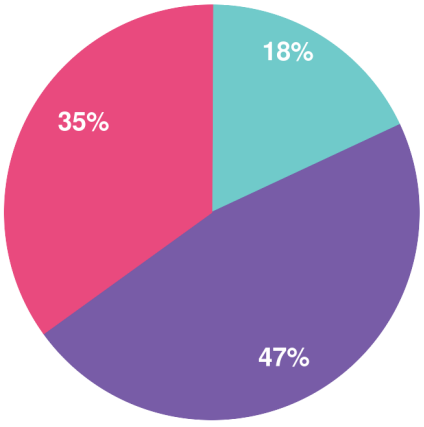
by visitors reading reviews

Construction Company	41%
University	21%
Manufacturing Company	7%
Outsourcing 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 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