aws marketplace

F5 Rules for AWS WAF

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

F5 Rules for AWS WAF

F5 Rules for AWS WAF Recap

F5 Rules for AWS WAF provides advanced web application protection tailored to secure applications hosted on AWS, offering dynamic defenses against evolving threats.

This solution offers a robust set of rules designed to enhance AWS WAF capabilities, delivering specialized protections against complex web threats. F5 Rules dynamically guard against emerging vulnerabilities, ensuring comprehensive threat mitigation. It's crafted to integrate seamlessly with AWS environments, making it fast and easy to deploy, manage, and scale as compared with legacy alternatives, providing users a manageable and comprehensive security layer for their applications.

What are the key features of F5 Rules for AWS WAF?

- Automatic Updates: Regularly refreshes its defenses to address the latest threats.
- Pre-built Rules: Offers a library of pre-configured rules that are easy to deploy.
- Scalable Configuration: Adapts seamlessly to changing web traffic conditions.

What ROI should users expect from F5 Rules for AWS WAF?

- Improved Security Posture: Reduces risk exposure with specialized threat intelligence.
- Cost Efficiency: Lowers operational costs by reducing the need for manual threat management.
- Time Savings: Streamlines deployment and maintenance with quick setup and automated updates.

In industries such as finance, healthcare, and retail, F5 Rules have been implemented to protect sensitive data and online transactions. This helps ensure compliance with industry regulations while maintaining performance and uptime for web applications.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- “Overall, the combination of reduced manual effort, improved security posture, and better application performance has delivered a strong return on investment.”

Vibin Thomas

Team Lead, Technical Content Security at Valuepoint Systems

- “I advise anyone looking for a great tool to secure their public-facing applications to start using F5 Rules for AWS WAF.”

Manmohan Rao

Associate Vice President at Hitachi Systems India Private Limited

- “F5 Rules for AWS WAF has positively impacted our organization for security through the implementation of traffic rules in our application.”

G Verduci

Consultant at a tech vendor with 10,001+ employees

What users had to say about valuable features:

"I really appreciate the way F5 Rules for AWS WAF generate reports proactively to show the number of exploits that come in and what remediation has been followed to block such exploits, mainly in the OWASP rule sets.

It has generated value toward us because since these e-commerce websites could become exposed to the public in an unsecure manner, which really no one wants. Now, looking at these rule sets, they ensure that our origin or our application content and code, as well as the application itself or its API, are secure enough, always.."

Manmohan Rao
Associate Vice President at Hitachi Systems India Private Limited

Read full review

"One of the best features of F5 Rules for AWS WAF is the advanced, continuously updated threat intelligence provided by F5. F5 Rules for AWS WAF rule sets are highly effective in detecting and mitigating OWASP Top 10 attacks such as SQL injection, XSS, and command injection, which significantly strengthens application security. Another key feature is the ease of integration with AWS WAF, allowing organizations to deploy enterprise-grade protection without additional infrastructure.

F5 Rules for AWS WAF can be quickly enabled and tested in count mode, which helps in safely evaluating their impact before enforcing them in block mode. F5 Rules for AWS WAF flexibility in tuning and customization is also a major advantage. Security teams can create exclusions, adjust the sensitivity, and combine F5 Rules for AWS WAF with custom AWS WAF rules to align with application-specific requirements and reduce false positives. Additionally, the visibility provided through AWS WAF logging and metrics helps in identifying attack patterns and making data-driven security decisions.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

“The best features F5 Rules for AWS WAF offers, from what I've seen or read so far, are application layer protection.

“I am referring to application layer protection with F5 Rules for AWS WAF, which stands out to me as using something similar to iRules to protect applications.

“F5 Rules for AWS WAF has positively impacted our organization for security through the implementation of traffic rules in our application.

“I have noticed specific benefits such as easy management with F5 Rules for AWS WAF, but I think that it's too early to provide a definitive assessment because I started using it only a few days ago..”

G Verduci
Consultant at a tech vendor with 10,001+ employees

Read full review

Other Solutions Considered

“We previously used AWS native rule sets and Fortinet rule sets. We switched to F5 Rules for AWS WAF because we found it more competitive. They continuously improve their security rules and keep adding vulnerability protection to their existing rule sets, ensuring we are protected and our applications are safe.

We mainly evaluated AWS native rule sets prior to F5 Rules for AWS WAF..”

Manmohan Rao
Associate Vice President at Hitachi Systems India Private Limited

Read full review

“Prior to using F5 Rules for AWS WAF, I was primarily relying on the default AWS managed rule sets and some custom WAF rules for application protection. While this provided a basic level of security, I found that they lacked the depth and advanced threat intelligence needed to effectively handle more sophisticated attacks and evolving threat patterns.

I switched to F5 managed rules to enhance my detection capabilities, especially for OWASP Top 10 vulnerabilities and more complex attack signatures. The continuous updates and better coverage helped me to improve my security posture. Additionally, using F5 Rules for AWS WAF reduced the need for frequent manual rule creation and tuning, making operations more efficient and scalable for enterprise environments..”

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"Before choosing F5 Rules for AWS WAF, I evaluated multiple options, including the default AWS managed rule sets, other AWS Marketplace alternatives, and other third-party WAF solutions such as Cloudflare and Akamai. The default AWS rules were easy to use but lacked the advanced threat coverage and depth in detection. Other third-party solutions provided strong capabilities, but integrating them into my existing AWS native architecture required additional effort and complexity.

I chose F5 Rules for AWS WAF because it offered a good balance between advanced threat intelligence, seamless integration with AWS WAF, and ease of deployment through AWS Marketplace. This allowed me to enhance security without adding operational overhead or changing my existing architecture significantly.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

ROI

Real user quotes about their ROI:

"It has absolutely saved money for our security team and time. There are two ways: either we write our own rule sets, which demands significant time, or we can use a more mature tool like F5 Rules for AWS WAF, which has already created these rule sets for perfect use cases like we are using for our end customers. Using F5 Rules for AWS WAF saves us time spent on developing security rules ourselves.."

Manmohan Rao
Associate Vice President at Hitachi Systems India Private Limited

Read full review

"I have seen a clear return on investment after implementing F5 Rules for AWS WAF. From a security perspective, I observed around 35 to 45% reduction in malicious application layer traffic reaching the origin, which helped protect the backend systems and reduce risk exposure. In terms of operational efficiency, the use of managed rules reduced manual effort by approximately 35 to 45% as many common threats were automatically detected and mitigated without requiring continuous rule creation and monitoring.

This also translated into time savings for the security team, allowing them to focus more on proactive security improvements rather than reactive incident handling. Additionally, by reducing unnecessary traffic and attack load, I saw improvements in application stability and performance, indirectly contributing to better user experience and reduced downtime risk. Overall, the combination of reduced manual effort, improved security posture, and better application performance has delivered a strong return on investment.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Use Case

“I have been using F5 Rules for AWS WAF for a short time and want to discover more about it.

“My main use case with F5 Rules for AWS WAF is testing it out.

“I don't have a quick specific example of what I'm testing at this moment.

“For now, I don't have anything else to add about my testing experience so far..”

G Verduci
Consultant at a tech vendor with 10,001+ employees

Read full review

"F5 Rules for AWS WAF provides advanced protection for web applications hosted on AWS against application layer attacks. I primarily use these rules to detect and block common threats such as SQL injection, cross-site scripting, remote code execution attempts, and other OWASP Top 10 vulnerabilities. F5 Rules for AWS WAF managed rule sets enhance AWS WAF's native capabilities by providing continuously updated threat intelligence and more granular signature-based detection.

In addition, I use these rules to handle automated and bot-driven attacks and traffic by identifying suspicious request patterns and reducing the unwanted traffic reaching the origin. This helps improve both security and application performance. From an operational perspective, the rules are initially deployed in count mode to analyze the traffic behavior, followed by tuning and gradual enforcement in block mode to minimize false positives and avoid business impact.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"We are providing support to our end customers who have e-commerce websites that need to be exposed to the public, and for a secure way around, we thought of getting them exposed via the Application Load Balancer to make sure it is exposed at Layer 7 only. While making sure it will be protected, we started using AWS WAF services, where we found that we can utilize a WAF rule set from Marketplace. We started using it, and I got the chance to be part of one of the summits where I heard of F5 Rules for AWS WAF. Since then, I have been using their rule sets for bot protection, web exploit OWASP rules, common vulnerabilities and exposures, and API security, which is a use case we are using to configure these rule sets.

We are using AWS WAF, which has been integrated with the Application Load Balancer to ensure that our Application Load Balancer is secure while it gets publicly exposed.

We thought of starting to use F5 Rules for AWS WAF primarily for DDoS protection nowadays, as AWS native rule sets also provide some protection for DDoS. I found that it demands continuous improvement in these rule sets. Previously, we used native rule sets, but these continuous demands were not listed in it, which led us to an unsecure environment. Now, using F5 Rules for AWS WAF for bot protection, I found that they continuously perform vulnerability scans while these rules come into action. This continuous improvisation ensures that I can build trust against these rules instead of other third-party rule sets.."

Manmohan Rao
Associate Vice President at Hitachi Systems India Private 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.

"I purchased and deployed F5 Rules for AWS WAF through AWS Marketplace, which made the onboarding and integration process straightforward and efficient.."

Vibin Thomas

Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Customer Service and Support

"I have reached out to customer support multiple times, especially while configuring rule sets for the first time. The support provided was excellent. I appreciate the assistance; they clearly explained everything, how to configure these rule sets, and what the best options are based on my use case, which helped us shortlist what is required.."

Manmohan Rao
Associate Vice President at Hitachi Systems India Private Limited

Read full review

"My customer support experience has been generally positive, especially when working through F5 and AWS together. For critical issues, the response time is quite good, and the support teams are knowledgeable in handling rule tuning, false positives, and other security-related incidents. One of the strengths is the availability of detailed documentation and predefined rule sets, which reduce the dependency on support for most common use cases.

However, for more advanced tuning or complex scenarios, I occasionally rely on vendor support, and they have been responsive and helpful. Overall, the support is reliable, but having more proactive recommendations or faster turnaround for complex cases would make it even better.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Other Advice

“I would advise not relying only on the default rule sets in blocking mode immediately. It is better to start in monitoring or count mode, analyze the traffic patterns, then gradually move to enforcement. Additionally, I recommend investing time in proper rule tuning, especially for critical applications such as login, APIs, or payment flows because false positives can impact business functionality if not handled carefully. Finally, ensure that logging and visibility are properly enabled from day one, so you can continuously improve the rule set based on real traffic and evolving threats. I would rate this solution as an 8 out of 10..”

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

“It's too early to provide my experience or advice to others looking into using F5 Rules for AWS WAF.

“I don't have any additional thoughts about F5 Rules for AWS WAF before we wrap up.

“I found this interview at AWS re:Invent.

“I gave this review a rating of 8..”

G Verduci
Consultant at a tech vendor with 10,001+ employees

Read full review

"I advise anyone looking for a great tool to secure their public-facing applications to start using F5 Rules for AWS WAF. These are managed rule sets, so you do not need to worry about continuous improvements or ensuring your application is secure; F5 Rules for AWS WAF will take care of that and is always making the necessary improvements in these rule sets to ensure security.

I am very impressed with the rule sets and the continuous engineering from their security team to ensure the required rule set availability. I really appreciate the fantastic job they are doing.

F5 Rules for AWS WAF can be integrated with AWS CloudFront, Application Load Balancer, Lambda, and API Gateway. I am satisfied with all these services as they are our intermediary points for services exposed to the public or globally.

I gave this product a rating of ten out of ten.."

Manmohan Rao
Associate Vice President at Hitachi Systems India Private Limited

Read full review

Top Industries

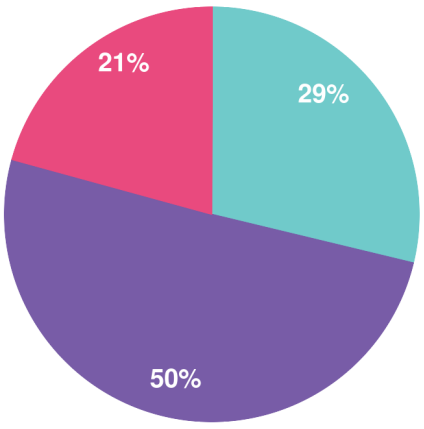
by visitors reading reviews

Construction Company	42%
Comms Service Provider	16%
Energy/Utilities Company	6%
Transportation Company	5%

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