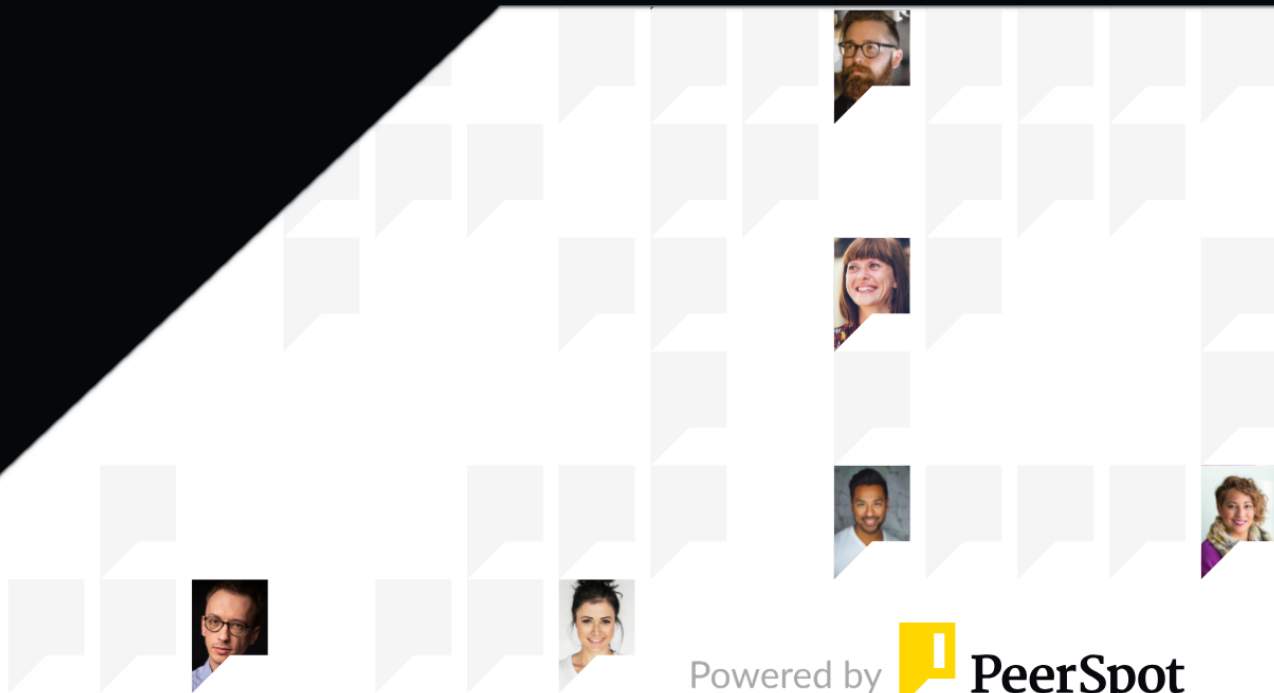




F5 Rules for AWS WAF

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 14

ROI..... 15 - 18

Use Case..... 19 - 23

Setup..... 24 - 25

Customer Service and Support..... 26 - 27

Other Advice..... 28 - 32

Trends..... 33 - 34

About PeerSpot..... 35 - 36

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

Technical Team Lead - Content Security at Valuepoint Systems

- ✓ “F5 Rules for AWS WAF is a strong, enterprise-focused solution for organizations that need robust web application security, centralized policy management, and better visibility into application layer threats within AWS environments.”



Sumanth Chowdary

Senior Technical Consultant at a tech consulting company with 5,001-10,000 employees

- ✓ “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 us by improving our web application security without adding too much operational overhead.”



Isaac Hernandez

Senior Technical Lead QA at a computer software company with 501-1,000 employees



“After implementing F5 Rules for AWS WAF, we observed a reduction of approximately 60 to 70% in web application security incidents reaching our application team, particularly blocking common threats like bot traffic and SQL injections without impacting our downstream systems.”



Pranav Telang

DGM at Airtel Digital



“F5 Rules for AWS WAF's OWASP protection and bot protection have reduced attacks on my applications by 72 to 90%.”



Harsh Goenka

Cloud Architect at a outsourcing company with 51-200 employees



“F5 Rules for AWS WAF is definitely recommended. It is a good tool for anyone to try and see if it matches their use case, and it is something that an organization can really benefit from.”



Ayodeji Bayo-Makinde

Technical Support Engineer at Horizon/Bespoke Labs

What users had to say about valuable features:

“Easy AWS integration is one of the best features F5 Rules for AWS WAF offers. The easy AWS integration can be attached to existing AWS WAF deployments within minutes and works with CloudFront application load balancers and APIs, which has improved our team's workflow..”

Iurii Efimov

Head Of Product & Engineering (Cpto) at a real estate/law firm with 11-50 employees

[Read full review](#) 

“The best features F5 Rules for AWS WAF offers include the pre-managed rules which help us identify the kind of traffic we receive from the external side, enabling us to adjust the sub-order rules to block CAPTCHAs or challenges to distinguish between legitimate traffic and possible bots.

“F5 Rules for AWS WAF integrates seamlessly with our AWS WAF, protecting our application load balancer, and it provides automation benefits by incorporating F5 managed rules deployment into our infrastructure as code in our CI/CD pipeline. This reduces the operational burden on our security team by automatically addressing issues. F5 Rules for AWS WAF has positively impacted our organization by improving our security posture and reducing the operational efforts of our security team in managing WAF policies. After implementing F5 Rules for AWS WAF, we observed a reduction of approximately 60 to 70% in web application security incidents reaching our application team, particularly blocking common threats like bot traffic and SQL injections without impacting our downstream systems..”

Pranav Telang

DGM at Airtel Digital

[Read full review](#) 

“The top features that F5 Rules for AWS WAF offers are its strong Layer 7 application protection capabilities, advanced traffic inspection, and flexibility in managing security policies for web applications and APIs. One major strength is protection against OWASP Top 10 threats such as SQL injection, cross-site scripting, and malicious bot activity through managed and customizable rule sets. The visibility and analytics around application traffic are also very valuable because they help security teams identify suspicious behavior and respond more proactively. Another strong feature is the integration with AWS environments, which makes deployment and scaling more streamlined for cloud-native applications. I also think the granular policy tuning and reduced false positives are important advantages because they help maintain security without significantly affecting legitimate user traffic. Overall, it provides a strong balance between security depth, operational control, and enterprise-grade application protection.

“One additional feature I find valuable is the visibility and reporting capability about application layer traffic and attack patterns. Having clearer insights into blocked requests, abnormal traffic behavior, and threat trends helps security teams make faster and more informed decisions. I also appreciate the scalability and flexibility of the solution in AWS environments because it supports both security and operational requirements without adding too much management complexity. Overall, the combination of strong protection, customization, and visibility makes the platform very practical for enterprise web applications..”

Sumanth Chowdary

Senior Technical Consultant at a tech consulting company with 5,001-10,000 employees

[Read full review](#) 

“The best feature that I appreciate about F5 Rules for AWS WAF is the dedicated API security where you can implement XML and JSON-based payload inspection. You have OWASP protection, including cross-site scripting and SQL injection prevention. Advanced bot protection is available to guard against web scrapers, system bots, and DDoS tools. F5 Rules for AWS WAF also provides CVE-specific protections, and because F5 manages those rules, they are continuously updated and managed. Easy integration with AWS services such as CloudFront or load balancers and enterprise-level threat intelligence are also provided.

The most important feature I would say is the OWASP protection that it provides.

F5 Rules for AWS WAF's OWASP protection and bot protection have reduced attacks on my applications by 72 to 90%. Almost all attacks are detected earlier, and because of its bot protection, my sites are not getting overloaded and clients are able to browse the application without bots requesting my load balancer and consuming excessive resources.

I have access to the load balancers' CloudWatch metrics from F5 Rules for AWS WAF, which shows how many requests are being received and how many unique users I have. I can list requests based on the WAF and determine how many IP addresses are requesting my load balancer. Through load balancer logs and metrics, I can confirm that attacks have been reduced by 72 to 90%..”

Harsh Goenka

Cloud Architect at a outsourcing company with 51-200 employees

[Read full review](#) 

“F5 Rules for AWS WAF offers very strong protection against common web attacks, including DDoS attacks. The rules are frequently updated on the WAF, and it provides enterprise-grade threat intelligence. This helps to proactively prevent threats even before they happen and reduces operational burden on the organization's part by reducing the need to set rules manually.

“The automatic rule updates in F5 Rules for AWS WAF help because the team does not have to worry about keeping up to date with the latest threats that come up in the web space. F5 handles figuring out and updating the rules to match current threats. This eliminates the need to evaluate and spend time determining which rules need to be updated for better threat protection.

“F5 Rules for AWS WAF has greatly helped to positively reduce operational burden because previously dedicated resources were required to update WAF rules. Although specific time metrics are not available, F5 Rules for AWS WAF has greatly reduced the resources allocated to putting in rules, freeing up those resources to handle other tasks and thereby helping to improve efficiency.

“Employees' time has been saved with F5 Rules for AWS WAF. Without F5 Rules for AWS WAF, some employees would need to be put in charge of setting up the rules on the WAF and then updating them. Since those resources no longer need to be dedicated to that task, they can be moved to deal with other work, thereby helping to increase efficiency..”

Ayodeji Bayo-Makinde

Technical Support Engineer at Horizon/Bespoke Labs

[Read full review](#) 

“In my opinion, the best features F5 Rules for AWS WAF offers include fast protection by managed rules, easy implementation, senior vulnerability management, and the necessary scanning for our team, which can range from more standard to reactive, allowing us to wait for an answer while we're loading the problem on the firewall.

“Mostly, I mean both easy implementation and customization. From the implementation side, it is a straightforward deployment.

“F5 Rules for AWS WAF makes my team's life easier because they can focus on new features and not spend as much time reviewing security requirements. In this case, I can say that having the lock or control in the log is great.

“One feature that we appreciate about F5 Rules for AWS WAF is the visibility through the AWS WAF logs. I will also highlight that combining F5 Rules for AWS WAF Managed Rules with custom AWS rules gives us a good balance for our specific applications.

“F5 Rules for AWS WAF has positively impacted us by improving our web application security without adding too much operational overhead.

“The main improvements we noticed with F5 Rules for AWS WAF include reducing malicious traffic, better visibility, and more confidence.

“The workload decreases mainly in analyzing malicious traffic thanks to F5 Rules for AWS WAF..”

IsaacHernandez

Senior Technical Lead QA at a computer software company with 501-1,000 employees

[Read full review](#) 

Other Solutions Considered

“Other options were not really evaluated before choosing F5 Rules for AWS WAF. What was wanted was known, and F5 Rules for AWS WAF checked all the boxes..”

Ayodeji Bayo-Makinde

Technical Support Engineer at Horizon/Bespoke Labs

[Read full review](#) 

“I previously used a standard AWS rule set before switching to F5 Rules for AWS WAF. I evaluated a standard AWS managed rule set before upgrading to F5 Rules for AWS WAF..”

Iurii Efimov

Head Of Product & Engineering (Cpto) at a real estate/law firm with 11-50 employees

[Read full review](#) 

“I was using native tools only before F5 Rules for AWS WAF, and sometimes I used other open source WAF providers. However, those open source tools, being free, do not have the capabilities at an enterprise level. Thus, I chose to move to F5 Rules for AWS WAF..”

Harsh Goenka

Cloud Architect at a outsourcing company with 51-200 employees

[Read full review](#) 

“Before using F5 Rules for AWS WAF, we mainly used native AWS WAF managed rules and some custom WAF rules. We switched because F5 Rules for AWS WAF gave us stronger managed security..”

IsaacHernandez

[Read full review](#) 

Senior Technical Lead QA at a computer software company with 501-1,000 employees

“I did evaluate other options before choosing F5 Rules for AWS WAF. I evaluated native AWS security tools including AWS Network Policies, Firewall Policies, Control Tower at the organizational level, AWS WAF, and AWS Shield..”

Harsh Goenka

[Read full review](#) 

Cloud Architect at a outsourcing company with 51-200 employees

“Before choosing F5 Rules for AWS WAF, I evaluated a few other options, including native AWS WAF capabilities and some other enterprise-range web application security platforms. The evaluation mainly focused on protection effectiveness, policy flexibility, operational visibility, scalability, and ease of managing application layer security across a cloud environment. F5 stood out for me because of its strong enterprise-grade security capabilities, advanced traffic inspection, customization flexibility, and centralized management approach. This aligned better with my operational and security requirements..”

Sumanth Chowdary

[Read full review](#) 

Senior Technical Consultant at a tech consulting company with 5,001-10,000 employees

ROI

Real user quotes about their ROI:

“We noticed ROI with F5 Rules for AWS WAF. F5 Rules for AWS WAF includes a lot of content, so in this case, I will estimate it simplifies our life and reduces the security work on common web attack patterns..”

IsaacHernandez

Senior Technical Lead QA at a computer software company with 501-1,000 employees

[Read full review](#) 

“After implementation, we saw a reduction of 40 to 50% in time spent by our security team, as the managed rule sets maintained by F5 significantly reduced the manual effort in administration while enhancing protection against common web attacks..”

Pranav Telang

DGM at Airtel Digital

[Read full review](#) 

“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 did see a return on my investment with F5 Rules for AWS WAF because I was able to detect attacks earlier, and because of this, my resources were not scaling continuously, thus saving costs on resources. Secondly, the client had a good experience because the application was not slow, which was previously happening because of continuous bot requests. Additionally, I now do not need many people checking the environment; I have AI capabilities and a few-member team can use those to help us out..”

Harsh Goenka

Cloud Architect at a outsourcing company with 51-200 employees

[Read full review](#) 

“We did see a return on investment after implementing F5 Rules for AWS WAF. There was a positive operational and security-related return on investment after implementing the solution. One measurable benefit was a reduction in manual effort required for managing and tuning web application protection policies because the managed rule capabilities and centralized visibility simplified the day-to-day operations. We also saw faster identification and response to suspicious application layer traffic, which improved operational efficiency for the security team. From a risk reduction perspective, the platform helped strengthen protection against common web attacks and reduced the likelihood of security incidents impacting public-facing applications. While exact financial metrics varied depending on workloads and application scale, overall I observed improvements in security consistency, reduced operational overhead, and better efficiency in managing web application security across AWS..”

Sumanth Chowdary

Senior Technical Consultant at a tech consulting company with 5,001-10,000 employees

[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

Technical Team Lead - Content Security at Valuepoint Systems

[Read full review](#) 

Use Case

“F5 Rules for AWS WAF manages the security rule set by applying the rules and setting the block directly in AWS WAF to provide advanced protection against web application attacks, bots, threats, and some known vulnerabilities. This enhanced security coverage protects our product against all OWASP Top 10 attacks..”

Iurii Efimov

Head Of Product & Engineering (Cpto) at a real estate/law firm with 11-50 employees

[Read full review](#) 

“I am using F5 Rules for AWS WAF for security checks and to implement policies to filter out network traffic and block malicious traffic. In my environment, all traffic goes through these WAF protections, and I have one tool installed in a VM through which all traffic is routed. I have implemented WAF rules on top of that infrastructure, and I have some applications running behind a load balancer. I have configured WAF rules for those load balancers to stop SQL injection, prevent DDoS attacks, implement OWASP protection, and validate rules based on headers..”

Harsh Goenka

Cloud Architect at a outsourcing company with 51-200 employees

[Read full review](#) 

“My main use case for F5 Rules for AWS WAF is to strengthen our security posture for our public-facing application for one of our US-based clients hosted on AWS, enhancing protection against common web attacks without introducing significant operational complexity. A specific example of how we use F5 Rules for AWS WAF for our public-facing application is that it allows us to quickly extend the native capability of AWS WAF, helping us detect and mitigate common threats such as SQL injection attempts, cross-site scripting, malicious bots, and exploitation techniques. This solution reduces the effort to maintain custom signatures while still providing strong security coverage..”

Pranav Telang

DGM at Airtel Digital

[Read full review](#) 

“Our main use case for F5 Rules for AWS WAF is for our APIs.

“We use F5 Rules for AWS WAF to block common attack patterns such as cross-site scripting and SQL injection. For example, when requests contain a certain payload in the headers, the firewall can block or count them before they reach the application or endpoints. We usually start in count mode, review logs for false positives, and move the rules to block mode once we are confident that we're not affecting legitimate users.

“One unique way we use F5 Rules for AWS WAF is as part of our firewall control deployment when we're deploying a new application or API..”

IsaacHernandez

Senior Technical Lead QA at a computer software company with 501-1,000 employees

[Read full review](#) 

“F5 Rules for AWS WAF is mainly used for securing web applications to protect against web attacks, including common web attacks like DDoS and SQL injection.

“With a particular client use case, the client had a gateway or an app gateway into their application. F5 Rules for AWS WAF was placed in front of that application so that it screens traffic coming in. This way, it serves as the first point of contact when a client makes a request to the application, offering the first level of protection for the application.

“If the application is in development or you are trying to make the application only available to a specific set of people, you can streamline the rules in F5 Rules for AWS WAF to allow only a certain IP address range..”

Ayodeji Bayo-Makinde

Technical Support Engineer at Horizon/Bespoke Labs

[Read full review](#) 

“My main use case for F5 Rules for AWS WAF is strengthening web application security for internet-facing applications hosted on AWS. I mainly use F5 Rules for AWS WAF to improve protection against common Layer 7 attacks such as SQL injection, cross-site scripting, bot-driven activity, and other OWASP Top 10 threats. Another important use case is reducing the operational effort involved in manually managing and tuning WAF rules by leveraging managed protection policies and centralized visibility. It has also been useful for improving security governance and helping security teams respond more proactively to suspicious traffic patterns and application layer threats.

“A specific example of how I used F5 Rules for AWS WAF is protecting a public-facing web application hosted behind an AWS Application Load Balancer, where we were seeing repeated suspicious requests and bot-driven traffic targeting login and API endpoints. F5 Rules for AWS WAF helped strengthen protection by applying managed rule sets for OWASP threats, filtering malicious traffic patterns, and reducing false positives through rule tuning. It also improved visibility into attack attempts and helped the security team identify abnormal request behavior more quickly, which improved overall response efficiency and application security posture..”

Sumanth Chowdary

Senior Technical Consultant at a tech consulting company with 5,001-10,000 employees

[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.

“My experience with pricing, setup cost, and licensing for F5 Rules for AWS WAF was very straightforward because it's all included on the vendor's side..”

IsaacHernandez

[Read full review](#) 

Senior Technical Lead QA at a computer software company with 501-1,000 employees

“Pricing for F5 Rules for AWS WAF was fair for the going market rate. Setup was mostly seamless and not complicated. A good experience was had on that front..”

Ayodeji Bayo-Makinde

[Read full review](#) 

Technical Support Engineer at Horizon/Bespoke Labs

“The pricing for F5 Rules for AWS WAF is not very costly and is reasonable, with enterprises being able to afford the cost. The setup is very easy, and licensing is managed by another team with which I am not familiar..”

Rohit Racharla

[Read full review](#) 

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

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

Vibin Thomas

[Read full review](#) 

Technical Team Lead - Content Security at Valuepoint Systems

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](#) 

“The customer support experience has been very positive, especially for enterprise-level support scenarios involving deployment guidance, policy tuning, and troubleshooting. The support team generally demonstrates strong technical knowledge around application security and traffic management, along with the AWS integrations. Overall, the experience with customer support is completely positive for us..”

Sumanth Chowdary

Senior Technical Consultant at a tech consulting company with 5,001-10,000 employees

[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

Technical Team Lead - Content Security at Valuepoint Systems

[Read full review](#) 

Other Advice

“F5 Rules for AWS WAF has an accuracy of about 80 to 90% in blocking common threats, providing a good balance between security coverage and false positives.

“I advise others looking into using F5 Rules for AWS WAF to clearly understand their application traffic and security requirements before deployment to add significant value, and to consider leveraging F5's threat intelligence managed rules while implementing automation in policy management. I rate this product an 8 overall..”

Pranav Telang

DGM at Airtel Digital

[Read full review](#) 

“I rate F5 Rules for AWS WAF eight out of ten because of the improvement points I mentioned before. Regarding F5 Rules for AWS WAF's AI capabilities, I would say its governance and security are pretty high, so I give it a ten out of ten.

“I would say the accuracy and reliability of output for F5 Rules for AWS WAF are pretty high, as it's based on the data from my account. The accuracy and reliability are based on data from my own AWS account.

“I would recommend connecting it from the beginning instead of using standard AWS managed rule sets. My overall review rating for F5 Rules for AWS WAF is eight out of ten..”

Iurii Efimov

Head Of Product & Engineering (Cpto) at a real estate/law firm with 11-50 employees

[Read full review](#) 

“F5 Rules for AWS WAF's AI capabilities have not been interacted with much so far, but given the way the resource itself is structured, the security would be expected to be top-notch, and governance would be up to standard.

“F5 Rules for AWS WAF has not been interacted with much, but from what has been heard from others, it is quite good and up to standard. It is good enough for the prevailing standard right now.

“F5 Rules for AWS WAF is definitely recommended. It is a good tool for anyone to try and see if it matches their use case, and it is something that an organization can really benefit from. The overall review rating for F5 Rules for AWS WAF is seven out of ten..”

Ayodeji Bayo-Makinde

Technical Support Engineer at Horizon/Bespoke Labs

[Read full review](#) 

“The advice I would give to others looking into using F5 Rules for AWS WAF is to first clearly understand their own application security requirements, traffic patterns, and governance objectives before implementing F5 Rules for AWS WAF. The platform delivers the most value when an organization takes time to properly tune policies, monitor traffic behavior, and align security control with application architecture. I would also recommend starting with managed rule sets and gradually introducing more customized policies based on real application usage and threat patterns. Involving both security and application teams early in the deployment process is important because it helps reduce false positives and improve operational efficiency. Overall, organizations that actively monitor, optimize, and regularly review their WAF policies will get the best long-term value from the platform.

“F5 Rules for AWS WAF is a strong, enterprise-focused solution for organizations that need robust web application security, centralized policy management, and better visibility into application layer threats within AWS environments. The platform provides a good balance between protection depth, customization flexibility, and operational control, which is especially valuable for internet-facing applications and APIs. I would rate this solution an 8 out of 10..”

Sumanth Chowdary

Senior Technical Consultant at a tech consulting company with 5,001-10,000 employees

[Read full review](#) 

“I would give F5 Rules for AWS WAF a rating of 10 out of 10.

The reason I choose a rating of 10 for F5 Rules for AWS WAF is that I am already using it at an enterprise level, and the amount of rules and the level of rules they have is really good. I do not have to deep-dive into the rules configuration part; it saves time. Since it is managed by F5, it is trustable and advanced.

When we have those AI capabilities, I am completely aligned with the governance

and security for F5 Rules for AWS WAF. Those capabilities are secure and will adhere to the policies that AWS follows; no data will be used outside the client's environment and without the client's permission. When we talk about the AI capabilities, I am only reading the data; I am not exposing it, and I am not using it; I am just protecting the data. I am completely aligned with the governance and security.

The accuracy and reliability of output from F5 Rules for AWS WAF is really accurate and reliable. There is always a scope of false positives as that is what AI systems are based on. Those are things that are not yet improved, but overall, I am satisfied.

I would really advise others looking into using F5 Rules for AWS WAF to go with it if they are at an enterprise level; it would be really good for them to use. If they are not at the enterprise level, the cost can really affect the environment. However, if they are at an enterprise level and want to switch to an advanced solution, I would recommend F5 Rules for AWS WAF..”

Harsh Goenka

Cloud Architect at a outsourcing company with 51-200 employees

[Read full review](#) 

“I would rate F5 Rules for AWS WAF a nine out of ten.

“I chose nine out of ten because of the auto-update for new features and the preview log.

“Regarding F5 Rules for AWS WAF's AI capabilities, I would say that it is not mainly an AI platform.

“From a governance and security perspective, F5 Rules for AWS WAF is solid because we can manage rules, get notifications about rule updates, and see who made changes to the configuration, but I think that the governance could be more robust.

“I want to continue with F5 Rules for AWS WAF.

“For AI capabilities, I will not describe F5 Rules for AWS WAF as having them.

“My advice for others looking into using F5 Rules for AWS WAF is to start with count mode, not block mode. I rate F5 Rules for AWS WAF a nine out of ten overall..”

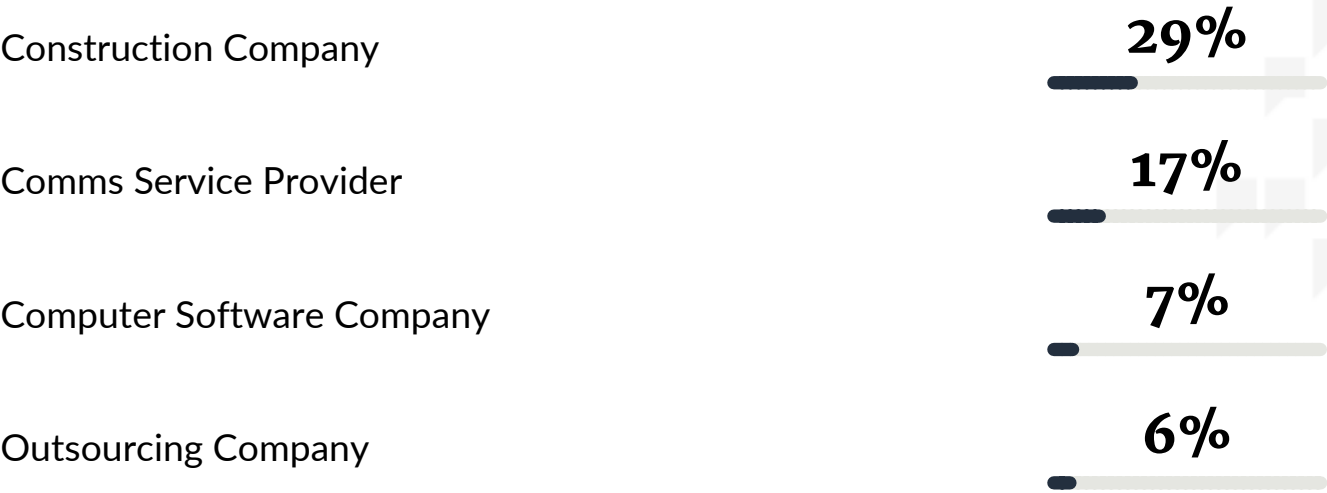
IsaacHernandez

Senior Technical Lead QA at a computer software company with 501-1,000 employees

[Read full review](#) 

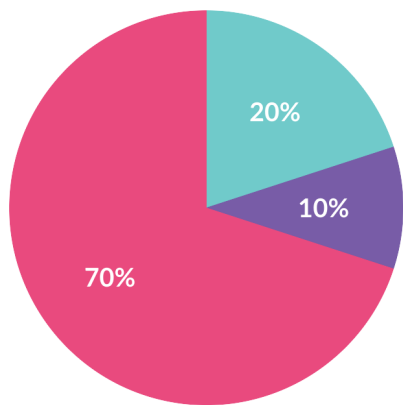
Top Industries

by visitors reading reviews

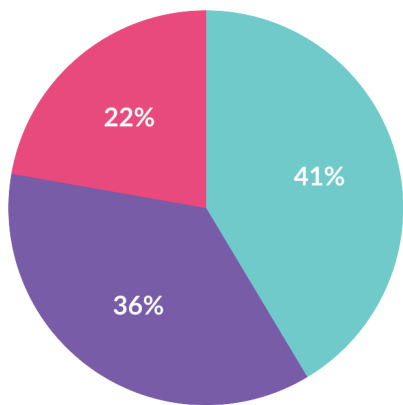


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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