aws marketplace

Fortinet Managed Rules for AWS WAF

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Fortinet Managed Rules for AWS WAF

Fortinet Managed Rules for AWS WAF Recap

Fortinet Managed Rules for AWS WAF enhances security by offering pre-configured firewall rules designed to protect AWS applications from common exploits and vulnerabilities.

Fortinet Managed Rules for AWS WAF offers advanced threat protection specifically tailored for the AWS environment. It seamlessly integrates with AWS WAF, providing security teams with a comprehensive solution to defend against sophisticated attacks without extensive configurations. The rules continually update to tackle the latest security challenges, affording peace of mind through effective threat mitigation.

What are the standout features?

- Automatic Updates: Ensures protection with constantly updated rules to tackle new threats.
- Pre-Configured Rules: Offers a collection of predefined rules designed for easy deployment.
- Seamless Integration: Direct integration with AWS services for streamlined security operations.

What benefits can users look for when evaluating?

- Reduced Management Overhead: Minimizes administrative time with automatic updates and simple integration.
- Enhanced Security: Provides robust protection against OWASP top 10 threats.
- Cost-Efficiency: Offers a comprehensive solution without the need for additional resources or expertise.

Fortinet Managed Rules for AWS WAF implementation is particularly beneficial in sectors like e-commerce and finance, where real-time threat protection is critical. These industries often face sophisticated cyber threats, and robust rule sets guard sensitive data, ensuring regulatory compliance and safeguarding customer trust.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Fortinet Managed Rules for AWS WAF has positively impacted my organization mainly by controlling the use of bots, as hackers and even ethical hackers feed data using them, helping us ensure that the traffic we are receiving is genuine and allowing us to analyze request times for each packet for great insight while automation saves time, lets me set geolocation rules, and track source IP behavior, which is very helpful for my organization."

Vivek Patoliya

IT Manager at Indic

- "Overall, Fortinet Managed Rules for AWS WAF has positively impacted our organization by strengthening application security, preventing cyber attacks, and ensuring regulatory compliance."

Rajeevkumar Rai

Associate Consultant at HCLSoftware

"Fortinet Managed Rules for AWS WAF provides positive feedback by protecting web applications and API protection while blocking advanced threats."

Mohan Janarthanan

Associate Vice President at Novac Technology Solutions

"After implementing Fortinet Managed Rules for AWS WAF, I observed measurable improvements, with around 70 to 90% of common web attack traffic blocked, a 60% reduction in application-level security alerts and incidents, and a substantial decrease in the time spent on WAF management from hours per week to near zero."

AravindR

Tech Lead at Exologic

"Overall, Fortinet Managed Rules for AWS WAF help us strengthen security, reduce operational overhead, and improve deployment speed, making our WAF management more efficient and scalable."

Vibin Thomas

Team Lead, Technical Content Security at Valuepoint Systems

"We get the benefits of continuous threat intelligence updates with very strong network security."

ShahnawazAlam1

Am at Godrej Capital

"Fortinet Managed Rules for AWS WAF positively impacts my organization by providing protection, as I have seen improved security, easier management, and fewer attacks due to limiting the requests, and the service has protected many things from man-in-the-middle attacks, denial of service, and SQL server attacks."

Abdelattim Abdelattim

Security Administrator at EJADA

What users had to say about valuable features:

"One of the best features of Fortinet Managed Rules for AWS WAF is the automation of rule updates, which significantly reduces the need for manual intervention. The managed rule sets provide effective coverage for common OWASP Top 10 threats, SQL injection attempts, and malicious bot activity, helping strengthen baseline application security.

Bot control and traffic filtering capabilities have been particularly useful in ensuring that incoming traffic is legitimate, improving visibility into request behavior and reducing unwanted or suspicious activity. The ability to quickly apply policies such as geo-blocking and IP reputation checks through AWS WAF integration also saves time and simplifies daily operations. Overall, these features help balance strong security with lower operational overhead.."

Vivek Patoliya
IT Manager at Indic

Read full review

"Fortinet Managed Rules for AWS WAF is useful and easy to use and manage, as it can handle use cases for denial of service and limited access, and serve as an application firewall for controlling who can access the application from outside the organization.

"The best features Fortinet Managed Rules for AWS WAF offers include the ease of FortiManager, which allows me to manage multiple WAFs from a single dashboard. Having everything on one dashboard helps speed up my team's workflow and efficiency because with one dashboard, I am not moving to another, and it uses multiple links, making it protected and easy for operation and management.

"Fortinet Managed Rules for AWS WAF positively impacts my organization by providing protection. Since using Fortinet Managed Rules for AWS WAF, I have seen a positive impact, including improved security and easier management. I have noticed fewer attacks due to limiting the requests, or if someone tries a man-in-the-middle attack to steal the communication between the application and the end-user, as the service has protected many things from man-in-the-middle attacks, denial of service, and SQL server attacks.."

Abdelattim Abdelattim
Security Administrator at EJADA

Read full review

"OWASP Top 10 protection is the best feature. Bot protection includes credential stuffing, scraping bots, and API security. Machine learning protection, data loss prevention, SSL/TLS inspection, and integration with cloud platforms like AWS, Azure, and Google Cloud are key features of Fortinet Managed Rules for AWS WAF.

After using these features, we are seeing fewer attacks in our organization. Fewer attacks mean we have more visibility. Fortinet Managed Rules for AWS WAF protects web applications from common cyber threats, allowing us to see the type of attack occurring, such as cross-site scripting and OWASP Top 10 vulnerabilities. This helps prevent data breaches, improve application availability, ensure regulatory compliance, and protect the organization's reputation in front of leadership, users, and clients.

Improved security means protection from Layer 7 attacks, including SQL injection, cross-site scripting, command injection, and bot attacks. Better business continuity is achieved since we are providing high availability, so the application stays available always and the service remains stable. We protect sensitive data like customer information, payment data, login credentials, and business data. We maintain compliance with security regulations including PCI DSS, GDPR, and ISO 20001. Overall, Fortinet Managed Rules for AWS WAF has positively impacted our organization by strengthening application security, preventing cyber attacks, and ensuring regulatory compliance.."

Rajeevkumar Rai
Associate Consultant at HCLSoftware

Read full review

"The best features of Fortinet Managed Rules for AWS WAF are automatic protection against OWASP threats, real-time threat updates, easy integration with AWS WAF, and reduced manual effort through preconfigured rulesets.

"Automatic protection with Fortinet Managed Rules for AWS WAF helps block threats instantly without manual effort, and real-time updates ensure the application stays protected against new and evolving attacks.

"Additionally, Fortinet Managed Rules for AWS WAF offers easy rule customization, better visibility through logs, and helps reduce false positives while maintaining strong security.

"Fortinet Managed Rules for AWS WAF has positively impacted my organization by improving application security by blocking threats automatically, reducing manual effort, and ensuring consistent protection with real-time updates.

"It helped to reduce security incidents, save time by automating threat protection, and improved overall efficiency in managing web application security. It helped save time by reducing manual monitoring, lowered security risk, and improved efficiency by automating threat protection with minimal resources.."

Cscsd Cscsd
Pricing Executive

Read full review

"Fortinet Managed Rules for AWS WAF offers many features, starting with the API security rule set, which covers SQL injection, XSS, command injection, file inclusion, deserialization, and is particularly essential for API apps protecting against JSON payload manipulation, API abuse patterns, and injection via API parameters.

"Fortinet Managed Rules for AWS WAF API rules help with API security compared to other tools I have used. With Fortinet Managed Rules for AWS WAF API, there is no need to write complex custom rules, which contrasts with other setups where I must write JSON inspection rules and regex for payload validation, saving significant time in rule creation and testing, since Fortinet Managed Rules for AWS WAF understands API behavior patterns and automatically detects abnormal parameter changes and JSON injections, including bot detection, credential stuffing detection, and requires minimal maintenance due to continuous updates.

"Staging Mode with count-to-block feature of Fortinet Managed Rules for AWS WAF helps avoid breaking production traffic, as it allows for rule tuning before switching to block mode, and its visibility and logging offer detailed insights into triggered rules and malicious payloads, aiding incident investigation.

"Fortinet Managed Rules for AWS WAF has had a clear positive impact on my organization, with a significant reduction in attack traffic. I had frequently seen SQL injection attempts previously, and after enabling Fortinet Managed Rules for AWS WAF, a large portion was automatically blocked at the edge, resulting in fewer security incidents and reduced operational efforts.

"After implementing Fortinet Managed Rules for AWS WAF, I observed measurable improvements, with around 70 to 90% of common web attack traffic blocked, a 60% reduction in application-level security alerts and incidents, and a substantial decrease in the time spent on WAF management from hours per week to near zero.."

AravindR
Tech Lead at Exologic

Read full review

"One of the best features of Fortinet Managed Rules for AWS WAF is the depth and quality of the threat protection that it provides. The rule sets are regularly updated with FortiGuard Threat Intelligence, which helps in protecting against evolving threats such as SQL injection, XSS, bot attacks, and zero-day vulnerabilities, without requiring any constant manual tuning. Another key advantage is the ease of deployment with the integration with AWS WAF.

"Fortinet Managed Rules for AWS WAF offers strong, enterprise-grade protection with minimal effort. One of the biggest advantages is the integration of the FortiGuard Threat Intelligence, which ensures that rules are continuously updated to defend against the latest threats such as SQL injection, XSS, and emerging vulnerabilities. The rules are also well-optimized to reduce false positives, which is critical in production environments, while providing flexibility to fine-tune behavior using exclusion overrides, allowing security teams to balance protection and application availability.

"I would like to highlight how the threat intelligence updates have impacted my team. Since the rules are continuously updated, we do not have to manually track every new vulnerability or threat pattern, significantly reducing our operational effort and ensuring that we are always protected against the latest attack vectors without delays. The ease of deployment made a big difference; we were able to quickly onboard the application into AWS WAF, which helped us improve our security posture in a very short time. The consistency of protection across the application helped standardize our security approach; instead of creating custom rules for every application, we relied on these managed rules for a strong baseline and fine-tuned only where necessary.

"Fortinet Managed Rules for AWS WAF has had a very positive impact on my organization, especially in terms of improving my overall security posture and reducing the operational effort. One of the biggest benefits has been proactive threat protection, allowing us to protect our applications against common and emerging threats without having to manually track every vulnerability, giving us confidence that our applications are consistently secured. From an operational perspective, it significantly reduces the time and effort required for rule management. Instead of building and maintaining complex custom rules, we

leverage the managed rule set for a strong baseline and focus only on fine-tuning wherever necessary. This helps my team save time and improve efficiency, while also minimizing the risk related to false positives and downtime. The rules are well optimized, and with proper tuning, we maintain a good balance between security and application availability, which is critical for business continuity. Additionally, the visibility through AWS WAF logs allows us to better understand attack patterns and improve our response strategy over time. Overall, it enables us to achieve stronger, more consistent security while simplifying the operational side and allowing the team to focus on higher-value tasks.

"Fortinet Managed Rules for AWS WAF has had a very measurable positive impact on my organization, both in terms of security improvement and operational efficiency. From a security standpoint, we observe a noticeable reduction in web-based attack incidents reaching the application layer. Common threats such as SQL injection, XSS, and bot-driven attacks are effectively blocked at the WAF level itself, which reduces the burden on the back-end systems and incident response teams. Operationally, it helps us save a significant amount of time; earlier, a lot of effort was spent on creating and tuning the custom rules. With Fortinet Managed Rules for AWS WAF, we use them as a baseline and focus on fine-tuning, which reduces our rule management effort by around 40 to 50 percent, especially during the onboarding of any new application. We also see faster deployment timelines; new applications can be protected within hours instead of days, improving our overall security onboarding process. In terms of cost and efficiency, fewer incidents and reduced manual effort indirectly lead to cost savings, particularly by minimizing the downtime risk and reducing the need for continuous rule maintenance. The improved visibility from AWS WAF logs helps us identify attack trends and proactively adjust our security posture. Overall, Fortinet Managed Rules for AWS WAF help us strengthen security, reduce operational overhead, and improve deployment speed, making our WAF management more efficient and scalable.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Other Solutions Considered

"I have used F5 before. Now we have switched to Fortinet Managed Rules for AWS WAF. F5 is a bit costly in comparison to Fortinet Managed Rules for AWS WAF.."

Rajeevkumar Rai
Associate Consultant at HCLSoftware

Read full review

"I also evaluated options like AWS native managed rules and other third-party WAF rulesets, but I chose Fortinet for better threat intelligence, automation, and ease of management.."

Cscsd Cscsd
Pricing Executive

Read full review

"I previously relied on the native managed rule set of AWS WAF along with custom rules, switching to Fortinet Managed Rules for AWS WAF for advanced protection and reduced operational overhead.."

AravindR
Tech Lead at Exologic

Read full review

"Before selecting Fortinet Managed Rules for AWS WAF, I evaluated AWS native rules, Cloudflare, F5, and Imperva, but Fortinet Managed Rules for AWS WAF offered the best balance of security and operational efficiency.."

AravindR
Tech Lead at Exologic

Read full review

"Previously, we used an open-source solution based on pfSense, primarily due to budget constraints at the time. While it provided flexibility, it required significant manual configuration and ongoing management. As our environment matured, we moved to a managed solution to reduce operational overhead and improve consistency in application security.."

Vivek Patoliya
IT Manager at Indic

Read full review

"Before selecting Fortinet Managed Rules for AWS WAF, we evaluated other solutions such as Palo Alto and Sophos. These options provided strong security capabilities but typically required more complex deployment models or additional infrastructure and management overhead in a cloud-native AWS environment.

Fortinet Managed Rules integrated more seamlessly with AWS WAF and offered a simpler, managed approach to rule updates and ongoing maintenance. This made it easier to standardize web application security while reducing operational effort compared to the alternatives we reviewed.."

Vivek Patoliya
IT Manager at Indic

Read full review

ROI

Real user quotes about their ROI:

"I have only been using Fortinet Managed Rules for AWS WAF for the past eight months, so I believe I would need a year to comment on return on investment.."

Mohan Janarthanan
Associate Vice President at Novac Technology Solutions

Read full review

"I see a clear return on investment after seeing significant time savings, reduced risk, and lower infrastructure load, leading to cost efficiency without needing to scale the security team.."

AravindR
Tech Lead at Exologic

Read full review

"Return on investment through using Fortinet Managed Rules for AWS WAF is definitely positive. Since we are protecting our application from Layer 7 attacks and deadly attacks, it provides a strong return on investment by preventing costly security incidents such as data breaches, application downtime, and fraud. By blocking web attacks like SQL injection and cross-site scripting before they reach the application, we are now stopping attacks at the WAF. The organization can avoid financial losses from regulatory penalties and operational disruption. This significantly reduces the overall cost of security incidents compared to the cost of deploying the WAF.."

Rajeevkumar Rai
Associate Consultant at HCLSoftware

Read full review

"While it is difficult to quantify ROI strictly in terms of direct cost savings, we have seen positive returns through improved security posture and operational efficiency. Fortinet Managed Rules for AWS WAF reduced the time and effort required to manage and update WAF rules manually, allowing the team to focus on monitoring and response rather than constant tuning.

From a risk-reduction perspective, preventing web attacks and ensuring consistent application availability provides clear business value, even if the benefits are not always directly measurable in monetary terms.."

Vivek Patoliya
IT Manager at Indic

Read full review

"I have seen a clear return on investment after implementing Fortinet Managed Rules for AWS WAF. One of the biggest gains is in time savings and operational efficiency. The effort required for creating and maintaining custom WAF rules reduced by around 45 to 55 percent, allowing my team to focus more on monitoring and optimization rather than rule management. I also observe a reduction in security incidents reaching back-end systems as common threats such as SQL injection, XSS, or automated bot traffic are effectively blocked at the WAF layer. This helps reduce incident handling effort and improves overall system stability. In terms of deployment, I am able to onboard and secure new applications much faster, in many cases within hours instead of days, improving my overall delivery timelines. From a cost perspective, while there is an additional licensing cost, it is offset by reduced manual effort, faster deployment, and lower risk of downtime or security breaches. Overall, it provides strong value by improving both security and efficiency without increasing team size.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Use Case

"My main use case for Fortinet Managed Rules for AWS WAF is having the OWASP rule set in place so it can work with the latest kinds of attacks, mitigations, and all.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"I have been using Fortinet Managed Rules for AWS WAF for one year or more. The main use case for Fortinet Managed Rules for AWS WAF is that it protects from any malicious attack for URLs, including injection or SQL injection, limits requests for denial of service, or addresses middleware attacks.."

Abdelattim Abdelattim
Security Administrator at EJADA

Read full review

"My main use of Fortinet Managed Rules for AWS WAF is to protect web applications from common threats like SQL injection, XSS, and bot traffic. I use it to automatically detect and block malicious requests and improve overall application security. In addition to basic protection, I also focus on monitoring logs, tuning rules to reduce false positives, and improving overall application security performance.."

Cscsd Cscsd
Pricing Executive

Read full review

"Our primary use case is protecting public-facing web applications hosted on AWS against common web threats while reducing the effort required to manage custom WAF rules. We use Fortinet Managed Rules to enhance baseline AWS WAF protection, particularly for OWASP Top 10 vulnerabilities, malicious bots, and abnormal web traffic.

The managed rule sets help standardize application security across workloads fronted by AWS services such as Application Load Balancers and CloudFront, while allowing us to focus on operations rather than constant rule tuning.."

Vivek Patoliya
IT Manager at Indic

Read full review

"I have been using Fortinet Managed Rules for AWS WAF mainly for protection against common web attacks like SQL injection, cross-site scripting, and remote code execution, securing AWS workloads, including virtual patching, API and application protection, and continuous threat intelligence updates.

"In virtual patching with Fortinet Managed Rules for AWS WAF, it blocks an exploit at the WAF layer before the code fix, which is illustrated by a typical scenario where I have a web app running on Amazon EC2 with a discovered vulnerability, such as an SQL injection in the login API, where an urgent fix is required but takes days, allowing attackers to exploit it. By enabling Fortinet Managed Rules for AWS WAF group in WAF, SQLi detection and payload pattern blocking are provided, so malicious requests are blocked before reaching the app.

"A fintech app had a login endpoint vulnerable to SQLi, and with a three-day patch ETA, Fortinet Managed Rules for AWS WAF rules immediately blocked the SQLi patterns with no downtime, avoiding the need for a hotfix.."

AravindR
Tech Lead at Exologic

Read full review

“I am protecting our application from Layer 7 attacks, and we mainly use Fortinet Managed Rules for AWS WAF.

Let's suppose I want to protect my application from OWASP Top 10 vulnerabilities. For that, I also want to protect from SQL injection, cross-site scripting, common injection, and file inclusion attacks. For this type of attack, we use ports and scanners to identify the kind of attack, including DDoS attacks. I am using this web application firewall to protect my application.

The main use case is creating a policy and protecting applications. Fortinet Managed Rules for AWS WAF protects web applications from application-layer attacks such as SQL injection, cross-site scripting, and OWASP Top 10 vulnerabilities. It sits in front of the web server and inspects HTTP and HTTPS traffic to detect and block malicious requests. I work for an ISP, so we have some critical applications that need protection. To protect those applications, we have created different policies. I will not reveal my client's name or the type of product, but I can give an example of the architecture: client, then WAF, then the web server, then the application. From the WAF, we have created a policy to protect our web server from Layer 7 attacks.

Let's suppose I am using a REST API and I want to protect that API. We have created a policy for that, including JSON and XML request inspection, API abuse detection, and rate limiting. For this type of protection, we are using API security. We also use bot protection for credential stuffing, scraping bots, fake account creation bots, and automated login attacks. For this, we have created a policy and profiles within a security policy..”

Rajeevkumar Rai
Associate Consultant at HCLSoftware

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.

"Regarding installation, there are some challenges, such as setting the internal network IP and configuring it. You can deploy it on a VM, but it can be difficult to manage during the initial period.."

ShahnawazAlam1

Am at Godrej Capital

Read full review

"The initial setup was straightforward. We purchased Fortinet Managed Rules for AWS WAF through the AWS Marketplace, and enabling the managed rule sets within AWS WAF was simple. Since it integrates natively with AWS WAF, there was no additional infrastructure to deploy, and the configuration process was quick and easy to manage.."

Vivek Patoliya

IT Manager at Indic

Read full review

Customer Service and Support

"Customer support for Fortinet Managed Rules for AWS WAF is generally good with timely responses and helpful guidance, especially for setups and troubleshooting issues.."

Cscsd Cscsd
Pricing Executive

Read full review

"Customer support was very prompt. Whenever we needed assistance, we logged a case and there was an engineer to help us. I really appreciate the support provided by Fortinet.."

Rajeevkumar Rai
Associate Consultant at HCLSoftware

Read full review

"Our experience with customer service and technical support has been positive. When support was needed, responses were timely and knowledgeable, and issues were addressed efficiently. Overall, the support experience has been reliable and adequate for operational needs.."

Vivek Patoliya
IT Manager at Indic

Read full review

"My experience with customer support has been generally positive; the documentation and Fortinet resources are helpful, and the support response is good when needed. For more complex issues or tuning scenarios, support provides useful guidance, although response times can vary depending on the priority and complexity of the cases. Overall, the solution is both scalable and reliable, with good support that helps maintain and optimize deployments.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"I have dealt with Fortinet support, and I would say their technical support is good.

"I have taken FortiCare Elite, which allows me to receive support within 15 minutes.

"I would rate the support an eight out of ten.

"As of now, I am not facing many issues that they need to improve upon to reach a ten.."

Mohan Janarthanan
Associate Vice President at Novac Technology Solutions

Read full review

Other Advice

"I advise others looking into using Fortinet Managed Rules for AWS WAF that it is easy for deployment, easy for management, and easy for configuration. I would rate this product an eight out of ten.."

Abdelattim Abdelattim
Security Administrator at EJADA

Read full review

"I chose a rating of eight out of ten for Fortinet Managed Rules for AWS WAF because it provides strong automated security and ease of use, but there is still room for improvement in customization and detailed visibility.."

Cscsd Cscsd
Pricing Executive

Read full review

"I would rate Fortinet Managed Rules for AWS WAF **8 out of 10**.

My advice to other organizations would be to clearly assess their application security requirements and operational capabilities before selecting a WAF solution. Fortinet Managed Rules work well for teams looking to strengthen baseline web application security on AWS without taking on heavy rule-management overhead.

The combination of native AWS WAF scalability with Fortinet's managed threat intelligence provides a good balance between cloud-native simplicity and enterprise-grade security. For organizations that value ease of deployment, automated updates, and consistent protection, this solution is a strong and practical choice.."

Vivek Patoliya
IT Manager at Indic

Read full review

"Fortinet Managed Rules for AWS WAF have helped me in many scenarios.

"If someone is planning to use Fortinet Managed Rules for AWS WAF, I recommend starting in count mode, understanding the application and traffic, tuning for sensitive endpoints, and testing in lower environments.

"Fortinet Managed Rules for AWS WAF have been foundational for my security stack, providing a good balance between strong out-of-the-box protection and reduced operational overhead. I would rate my overall experience with Fortinet Managed Rules for AWS WAF as an eight out of ten.."

AravindR
Tech Lead at Exologic

Read full review

"I would recommend starting by using Fortinet Managed Rules for AWS WAF as a baseline protection layer rather than relying entirely on custom rule sets from the beginning. It helps quickly secure the application with minimal effort. I would also recommend enabling the rules initially in monitoring log mode, reviewing the traffic, and gradually moving to block mode. This approach helps in identifying and tuning false positives without impacting legitimate users. Another important point is to leverage AWS WAF logging and CloudWatch insights to understand traffic patterns and continuously fine-tune the rules based on application behavior. For organizations managing multiple applications, it is beneficial to standardize rule sets and apply them consistently across environments while allowing flexibility for specific exceptions. Overall, Fortinet Managed Rules for AWS WAF is very effective, but combining it with proper monitoring, tuning, and regular review will give the best results in terms of both security and performance.

"Overall, Fortinet Managed Rules for AWS WAF has been a reliable and effective solution for securing my application. It provides strong baseline protection with minimal effort and integrates well within the AWS WAF ecosystem. With proper tuning and monitoring, it offers a good balance between security and performance. While there are areas for improvement in visibility and advanced customization, the solution delivers solid value and scalability for organizations managing modern cloud workloads. I would rate this solution an eight out of ten.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"Analytics is helpful to me, including bandwidth usage per application or user consuming the bandwidth, traffic from the source IP or destination IP, and DNS information. Fortinet Managed Rules for AWS WAF has custom security policies which we can customize based on source or destination IP, users or groups, applications, service ports, and schedules based on time. We can also customize our application controls to detect priority applications, block applications, limit

applications, apply bandwidth on applications, and use custom IPS signatures to detect specific attack patterns, block unusual traffic behaviors, and protect internal applications. Custom web filtering categories can be created to allow or block specific websites, and we can control web access by users, determining which users can access which sites.

We get the benefits of continuous threat intelligence updates with very strong network security. We can integrate it with security platforms, and it offers high performance, centralized management, and advanced threat intelligence. We can access it securely with remote access, and it provides improved network visibility and cost efficiency.

The built-in analytics for real-time attack insights is good because we are using it. If I were to rate support from zero to ten points, I would give eight and a half points for their support. For Fortinet Managed Rules for AWS WAF, I would rate it the same, eight and a half points. I believe the overall solution would be closer to eight points. I would rate this product eight out of ten.."

ShahnawazAlam1
Am at Godrej Capital

Read full review

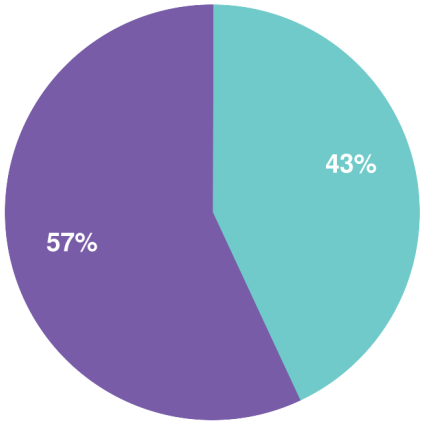
Top Industries

by visitors reading reviews

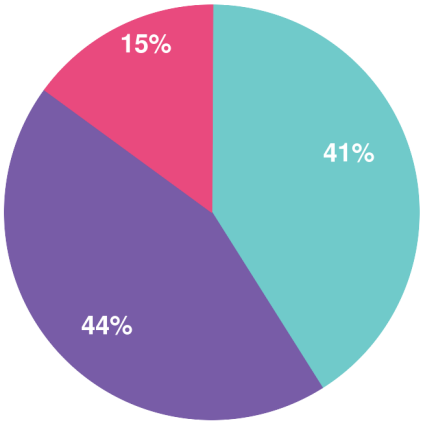
Construction Company	34%
Financial Services Firm	13%
Logistics Company	13%
Outsourcing Company	11%

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