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

Technical Team Lead at Exalogic Consulting

"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

"Fortinet Managed Rules for AWS WAF offers the best features by protecting my servers and blocking unauthorized access while also giving me the flexibility to only enable allowed access."

Kelghazouli Rasuli

Group IT Director at Premier Group

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

ShahnawazAlam1

Am at Godrej Capital

What users had to say about valuable features:

"The best features Fortinet Managed Rules for AWS WAF offers include regularly updated rules which incorporate the latest threat intelligence, logs, alerts, and the ability to block malicious requests that we have found on this WAF.

"Fortinet Managed Rules for AWS WAF positively impacts my organization by providing protections against API-based attacks, rule-based security, and threat intelligence from FortiGuard.."

HARISH JOGADIYA
Project Manager at Pentagon System and Services Pvt. Ltd.

Read full review

"Fortinet Managed Rules for AWS WAF offers the best features by protecting my servers and blocking unauthorized access while also giving me the flexibility to only enable allowed access.

"The flexibility it offers for enabling allowed access works for me as I have multiple websites on this server using multiple ports, so using port address translation allows us to publish only a specific website.

"Fortinet Managed Rules for AWS WAF has positively impacted my organization by decreasing the risk and vulnerability and the threats to attack my internal server.."

Kelghazouli Rasuli
Group IT Director at Premier Group

Read full review

"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

“Fortinet Managed Rules for AWS WAF is mainly used for controlling the use of bots and hackers, and tracking geolocation rules and source IP behaviors, which is very helpful in our application and organization from a security perspective.

“The main features include integration with AWS, Azure, and Google Cloud. Additionally, it helps protect against OWASP Top 10 vulnerabilities, helps prevent data breaching, and ensures regulatory compliance.

“Fortinet Managed Rules for AWS WAF has positively impacted us. We were not having financial losses because our application, the lockers, is where citizens place their parcels. Someone could potentially try to manipulate those devices. To protect against such security risks and penalties, this solution helped notify us about what is coming to our application from a hacker's perspective and how they are trying to exploit the application. To mitigate these things, it has been helpful for us.

“Since using Fortinet Managed Rules for AWS WAF, financial losses have gradually decreased. Because this is a customer-facing environment where citizens of Belgium use the lockers to place their parcels, we were able to mitigate this risk. Additionally, whenever a hacker was trying to exploit the system and asking for a bounty, that threat was completely eliminated. These two things are very valuable for our application to mitigate..”

Rohit Racharla

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

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
Technical Team Lead at Exalogic Consulting

Read full review

Other Solutions Considered

"I did not previously use a different solution, as this was the first time solution to do that, and after that, I have also used the WAF for Huawei Cloud.."

Kelghazouli Rasuli
Group IT Director at Premier Group

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
Technical Team Lead at Exalogic Consulting

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
Technical Team Lead at Exalogic Consulting

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 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
Technical Team Lead at Exalogic Consulting

Read full review

"For return on investment, since we are protecting our application from Layer 7 attacks and deadly attacks, Fortinet Managed Rules for AWS WAF helps us prevent data breaches and protects against hackers trying to exploit the lockers or someone trying to steal parcels from the lockers. For that, it has been very helpful.."

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

Read full review

"A general sense is that Fortinet Managed Rules for AWS WAF is decreasing our risk.

"I do not have an exact number or figures or metrics to share, but based on what we are checking on the logs, we find that multiple unauthenticated access attempts have already been blocked.."

Kelghazouli Rasuli
Group IT Director at Premier Group

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 to manage our rules and utilize its pre-configured security rules as an AWS WAF forensic provider.."

HARISH JOGADIYA
Project Manager at Pentagon System and Services Pvt. Ltd.

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

"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

"We are using Fortinet Managed Rules for AWS WAF for one of our front-end applications called the lockers application, where it will be interacted with our postmen in Belgium. For that application to protect against hackers and bots, we are using these WAF rules.

"Currently, I have used Fortinet Managed Rules for AWS WAF in the AWS service provider for cloud. We have integrated this in the WAF for the locker application, which is an end customer application, and we receive around thousands to hundreds of thousands of requests coming to our application. Since this is publicly exposed, we are using it to make our application more secure and robust without any downtime or security attacks.."

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

Read full review

"My main use case for Fortinet Managed Rules for AWS WAF is to use it as a firewall to protect my internal device which is in the internal network in AWS and the internet.

"To protect my internal device, I had some servers inside the internal network in AWS, one of which is a published server, a web server, that we would like to publish some of this website's application to users outside in our previous company. We have an application hosted in AWS that has a web interface accessible through multiple tablets connected to around 110 trucks all around Egypt, and we have used Fortinet Managed Rules for AWS WAF to publish only this website to a specific number of tablets.

"Regarding my main use case, we choose the right rule which is only publishing this web interface with a specific port, and we changed this port to a non-standard port to be able to be secured, and changing the port also decreases the threats usually aimed at the default ports for HTTP and HTTPS.."

Kelghazouli Rasuli
Group IT Director at Premier Group

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
Technical Team Lead at Exalogic Consulting

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

"I purchased Fortinet Managed Rules for AWS WAF through the AWS Marketplace.

"My experience with pricing, setup costs, and licensing is that I did not take a large amount or large package, so it is acceptable for me.."

Kelghazouli Rasuli

Group IT Director at Premier Group

Read full review

"I purchased Fortinet Managed Rules for AWS WAF through the AWS Marketplace, which is the only option available.

"Since it is present in AWS, the cost of Fortinet Managed Rules for AWS WAF is not high, and my customer is also happy with the cost and the work it is doing. At the integration level, it is a click and use solution.."

Rohit Racharla

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

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

"The customer support for Fortinet Managed Rules for AWS WAF was very prompt. Whenever assistance was needed, there was always an engineer available to help us. I really appreciate their support.."

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

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 would rate Fortinet Managed Rules for AWS WAF a seven out of ten. I highly recommend others to try Fortinet Managed Rules for AWS WAF and see how exactly these managed rules are working.."

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

Read full review

"I have no additional comments or advice to give to others looking into using Fortinet Managed Rules for AWS WAF. I have no additional thoughts about Fortinet Managed Rules for AWS WAF. I would rate this product a 10.."

HARISH JOGADIYA
Project Manager at Pentagon System and Services Pvt. Ltd.

Read full review

"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

"My advice to others looking into using Fortinet Managed Rules for AWS WAF is that it is reasonable, flexible, and cost-sufficient.

"In my point of view, Fortinet Managed Rules for AWS WAF is acceptable, as I did not face any issue or any complicated configuration. I gave this product a rating of eight out of ten.."

Kelghazouli Rasuli
Group IT Director at Premier Group

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
Technical Team Lead at Exalogic Consulting

Read full review

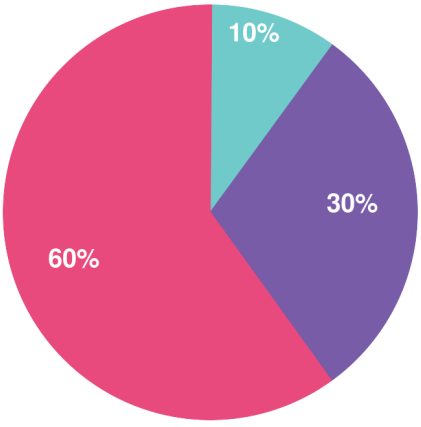
Top Industries

by visitors reading reviews

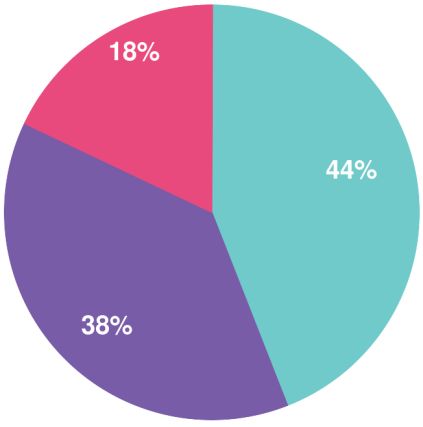
Construction Company	29%
Financial Services Firm	12%
Logistics Company	11%
Outsourcing Company	10%

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