aws marketplace

F5 Advanced 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 - 17

Use Case . . . . . 18 - 23

Setup . . . . . 24 - 26

Customer Service and Support . . . . . 27 - 28

Other Advice . . . . . 29 - 33

Trends . . . . . 34 - 35

About PeerSpot . . . . . 36 - 37

©2026 PeerSpot, All Rights Reserved

Product Recap

F5 Advanced WAF

F5 Advanced WAF Recap

F5 Advanced WAF delivers robust web security with features like signature-based threat protection and behavior analysis, ensuring app stability and security.

F5 Advanced WAF integrates advanced security with functionalities such as SQL injection defense and real-time threat intelligence. It enhances security for applications with load balancing, bot detection, and DDoS protection alongside comprehensive attack monitoring capabilities. Popular among diverse sectors, its usability and easy integration make it a practical choice by providing a stable security infrastructure across both on-premises and cloud environments.

What are the key features?

- Signature-Based Protection: Defends against SQL injections and other cyber threats with up-to-date signature detections.
- Behavior Analysis: Reduces false positives by monitoring patterns and behaviors.
- Load Balancing: Ensures application stability and optimal performance.
- Bot Detection: Identifies and mitigates bot traffic to secure applications.
- DDoS Protection: Guards against distributed denial of service attacks, maintaining service availability.
- Real-time Threat Intelligence: Offers live updates and insights into potential security threats.

What benefits and ROI can organizations expect?

- Enhanced Security: Comprehensive protection against an array of web-based threats.
- Improved Performance: Raises application availability and user experience.
- Deployment Flexibility: Supports diverse environments, from on-premises to cloud settings.
- Ease of Integration: Simple incorporation into existing security frameworks.

Particularly relevant in banking and financial services, F5 Advanced WAF safeguards applications from threats like SQL injections and DDoS attacks, ensuring compliance and API security. Its capabilities are leveraged for both load balancing and application defense, offering a versatile deployment model suited for protecting critical infrastructure in competitive and demanding industries.

©2026 PeerSpot, All Rights Reserved

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "After implementing F5 Advanced WAF, nearly 99.9% of requests are legitimate due to the granularity and response verification by attack patterns and request blocking."

  Validated user

  Senior Security Systems Engineer at a tech services company with 11-50 employees

- "Overall, F5 Advanced WAF is a strong, dependable enterprise solution that works best when seen as a long-term security platform rather than a quick add-on; once properly designed, sized, and tuned, it runs quietly in the background and effectively does its job without constant attention."

  Kallamuddin Ansari

  Cyber Security Consultant at HR Software Solution

- "The level of configurability that I get with F5 Advanced WAF solution is immense, and I have to be a bit aware of how it works and all of its features, but at the end of the day, it is all about the administration expertise that I will require to have and use it to my liking based on the kind of services that I have onboarded on my solution itself."

  Kkc Casey

  Security Solutions Architect at a consultancy with 1-10 employees

©2026 PeerSpot, All Rights Reserved

"Overall, I believe it has been a good decision to switch because I do not think any other product available on the market can compete with F5 at this time."

Pawan Thakur

Security Analyst at IBM

"F5 Advanced WAF offers features not available in other products."

Validated user

Global Channel Alliances Lead at a tech vendor with 10,001+ employees

"WAF functionality is valuable for protecting applications from attacks."

Ahmed Moamen

Senior Security Solutions Architect at Orange

"The AOF solution provides numerous security features."

Amr Shawky

Security & Infra Technology Specialist at BARQ Systems

©2026 PeerSpot, All Rights Reserved

What users had to say about valuable features:

"The whole mechanism of F5 Advanced WAF is effective. It contains the logic of both negative and positive security combined, providing added value to the company I work with to protect their applications.."

RoiNahari
CEO at CyberApp

Read full review

"The features of F5 Advanced WAF that I find most valuable include advanced WAF capabilities, bot detection, DDoS features, and all the top ten attacks we have configured with the WAF.

"Machine learning and automated threat detection features have helped our security strategy because we initially used them during our application learning mode. It provides us with one hundred percent accurate application learning to reduce false positives, and it has been very helpful.."

Pawan Thakur
Security Analyst at IBM

Read full review

©2026 PeerSpot, All Rights Reserved

"F5 Advanced WAF provides two different licensing models. The subscription-based model offers competitive pricing, making it easier for me to see ROI. However, the perpetual license, despite an initial higher cost, lacks transparency regarding support expiration. Due to the subscription, I can compare it with other tools, but as a perpetual buyer, I am unaware of support expiration until after the purchase, allowing indicative ROI calculations but not actual ones.

Furthermore, F5 Advanced WAF offers features not available in other products, though I suggest consulting a technical expert for specific features.."

Validated user

Global Channel Alliances Lead at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The best features F5 Advanced WAF offers include iRules, which are the most important, where out of the box requirements can be met, even if F5 Advanced WAF does not have them natively. If something is missing, iRules help achieve functionality that is lacking. This is the first standout feature against other vendors' products. The second most crucial feature is their secure traffic handling manager, which is stable and handles millions of requests within milliseconds. That is the most stable in the current market. Thirdly, the granularity of security policies, where we can segregate user and administrative policies on the same virtual server, is important. Additionally, the advanced bot protection is very good, with numerous categories of bots. Their DDoS protection also offers granularity, including behavioral DDoS features that verify server load. They incorporate client-side integrity by sending JavaScript to clients to determine whether they are real browsers or bots before verifying requests. There is also rate limiting in the DDoS features. Furthermore, they have session awareness features where if a single client generates a specified number of violations within a time frame, the IP can be automatically blocked for a specified period. These features stand out for F5 Advanced WAF compared to vendors in the market.

"F5 Advanced WAF has positively impacted my organization. We can lower down the attacks; there are ways the non-legitimate malicious requests can pass. However, after implementing F5 Advanced WAF, nearly 99.9% of requests are legitimate due to the granularity and response verification by attack patterns and request blocking.."

Validated user

Senior Security Systems Engineer at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"F5 Advanced WAF offers excellent configurability, and you have all the things in your hand that you want to configure for it. It starts from overall network level things to how a web application should be developed, for example, how an HTTP request should be created from the backend itself and how it is made an RFC compliant HTTP request. I can tune the configuration and security configurations based on each very minute content or minute context details. I can fine-tune my policy to act upon very specific parameters on very specific URLs and very specific headers.

Even if I get false positives, I can disable it for very specific contexts in an HTTP request and not on the whole application level because disabling a signature on a whole application level might not be that secure or recommended as it might cause false positives on specific input endpoints or on a specific area. The same kind of attack signature or the same kind of attack may be executed in another part of the same application which is covered by a single policy in itself. The level of configurability that I get with F5 Advanced WAF solution is immense, and I have to be a bit aware of how it works and all of its features, but at the end of the day, it is all about the administration expertise that I will require to have and use it to my liking based on the kind of services that I have onboarded on my solution itself.

F5 Advanced WAF has positively impacted my organization by providing immense visibility of the application traffic itself and how it protects against attacks that are prevailing in the application. The threat intelligence and threat campaigning feature that F5 provides allows their in-house threat intelligence team to research regularly and provide updates based on real-time or near zero-day attacks. The IP intelligence databases that it provides and the many other things F5 provides are something that I believe every organization should have in their security budget or security architecture. I think it is something that is a must-have solution. It does not matter if it is F5 or any other solution, but it should be enough to protect an organization from the threats that are prevalent in these generations, which require a really complicated solution itself, and F5 is one of them.."

Kkc Casey
Security Solutions Architect at a consultancy with 1-10 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"From my hands-on experience with F5 Advanced WAF in the banking production environment, some of the best features that really stand out are those that help reduce risk without breaking applications. One major strength is its Behavioral and Automatic Learning capabilities, which allow the WAF to understand normal application behavior and help create policies based on real traffic, minimizing manual effort and false positives. Another notable feature is the Advanced Attack Signature database that is very strong and regularly updated, effectively blocking SQL injections, cross-site scripting, command injections, and file inclusion attacks while allowing selective enabling or disabling of signatures to avoid blocking genuine traffic. Additionally, the Bot Protection feature is critical for the login page and API, helping stop automated login attempts, control scraping, and manage abnormal request rates, which ultimately reduces unnecessary loads on the backend server and improves overall stability. Finally, the strong visibility and logging properties provide detailed event logging and reporting, allowing the security team to see which attacks were blocked, which parameters or URLs triggered them, and source behavior patterns.

In my day-to-day activities, if I had to pick one feature I rely on the most within F5 Advanced WAF, it would be the Behavioral Learning with policy tuning, as the biggest challenge in application security, especially in the banking sector, is avoiding false positives. Applications frequently change, new parameters are added, and user behavior can evolve. This feature allows me to review newly learned parameter URLs and fine-tune enforcement so genuine users are not impacted, confidently moving policies from staging to blocking mode, saving significant time and preventing unnecessary production issues. In a large environment, security teams cannot manually write rules for everything, so this learning engine provides a baseline, allowing us to apply engineering judgment on top of it, which makes F5 Advanced WAF usable in real life. From a daily operation point of view, F5 Advanced WAF stands out because it is practical, stable, and predictable once properly tuned, which is exactly what you want in a critical enterprise environment.

F5 Advanced WAF has a clear and measurable positive impact in our organization, particularly regarding our security posture, application stability, and operational

©2026 PeerSpot, All Rights Reserved

efficiency. After implementing F5 Advanced WAF, we saw a significant reduction in web-based attacks such as SQL injection, cross-site scripting, and automated malicious traffic, allowing us to block real threats before they reached the backend server. With proper use of behavioral learning and tuning, false positives are greatly reduced, leading to minimal impact on genuine users and fewer application outages caused by security controls. This created higher confidence when running the policy in blocking mode, which was a big win for both the application and security team. Strong visibility and faster incident response through detailed logging and reporting help our team quickly identify patterns, perform faster root cause analyses, and support audit and compliance requirements, ultimately reducing investigation time and improving overall response efficiency.

After implementing F5 Advanced WAF in the enterprise banking environment, we saw measurable improvements across security and operations, including reduced web attacks, decreased false positives over time, improved application stability, faster incident response investigations, and operational efficiencies.."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

Read full review

©2026 PeerSpot, All Rights Reserved

Other Solutions Considered

"I recommend Infoblox because it's a leader in DNS security with more than 15 customers using it. It is very flexible in configuration, support, and scalability compared to F5.."

Amr Shawky
Security & Infra Technology Specialist at BARQ Systems

Read full review

"We chose this product because we believe it is the best product for us. There are other firewalls in the market, but you always look for the best as a vendor.."

Validated user
Technical Product Manager at a tech services company with 11-50 employees

Read full review

"Before choosing F5 Advanced WAF, I evaluated options like Imperva and Cloudflare. However, F5's reputation and stature built over the years is commendable and influenced my decision.."

Validated user
Senior Security Systems Engineer at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Before choosing F5 Advanced WAF, we evaluated other options such as Akamai, which is a cloud-based solution and not recommended for critical data in a cloud environment since it does not provide an on-premise solution.."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

Read full review

"I do not use a WAF solution in my end itself, but I do provide that solution to others. I have used FortiWeb and Imperva and Traceable to provide solutions to clients, but as of now, the on-premises solution is primarily F5, which is a bit better in this case. Imperva and Akamai are there if they provide on-premises solutions, but it is good enough in itself for now, at least.."

Kkc Casey
Security Solutions Architect at a consultancy with 1-10 employees

Read full review

"I switched from Radware to F5 Advanced WAF after COVID, which was two to three years ago.

"Overall, I believe it has been a good decision to switch because I do not think any other product available on the market can compete with F5 at this time.."

Pawan Thakur
Security Analyst at IBM

Read full review

©2026 PeerSpot, All Rights Reserved

ROI

Real user quotes about their ROI:

"I find it difficult to compute ROI for perpetual licenses due to the lack of upfront information about support expiry. Subscription models offer clearer ROI due to a more competitive pricing scheme.."

Validated user
Global Channel Alliances Lead at a tech vendor with 10,001+ employees

Read full review

"The ROI is very impressive as it is crucial for financial applications to be protected efficiently. Ensuring application security is a significant milestone, crucial to prevent financial losses or penalties.."

Amr Shawky
Security & Infra Technology Specialist at BARQ Systems

Read full review

©2026 PeerSpot, All Rights Reserved

"There are numerous benefits for end customers, as a secure application helps prevent potential breaches and ensures the safety of customers' data, especially in sensitive sectors like banking.."

Validated user
Senior Network Engineer at a comms service provider with 11-50 employees

Read full review

"In terms of return on investment with F5 Advanced WAF, if an administrator is good enough in operating a WAF solution, then a single administrator would work. The amount of attacks it protects against is immense, more than F5 Advanced WAF itself costs. So it is worth it to have.."

Kkc Casey
Security Solutions Architect at a consultancy with 1-10 employees

Read full review

"I have seen a return on investment with F5 Advanced WAF. The time saved is significant because of its learning feature, allowing automatic configuration for legitimate requests. This automatically accommodates changes, ultimately saving time. Additionally, the overall operational costs decrease as F5 Advanced WAF ensures 24/7 application availability, preventing any traffic disruptions impacting business operations. Hence, F5 Advanced WAF delivers a solid return on investment.."

Validated user
Senior Security Systems Engineer at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"We have seen a clear return on investment after deploying F5 Advanced WAF, primarily in terms of time and risk reduction. Time savings in daily operations come from the automatic learning and signature update reducing the need for constant manual rule management, allowing the security and network teams to spend significantly less time handling false positive application-related escalations. Incident investigation time was reduced because logs clearly indicate what was blocked and why, leading to faster resolution and more efficient use of existing engineers. A large volume of malicious traffic was blocked at the WAF layer, preventing issues from reaching the backend servers, which reduced emergency troubleshooting and application team involvement, ultimately lowering operational stress and incident cost savings without requiring additional security tools. This saved costs on hardware, licensing, integrations, and support effects, with the realistic ROI summarized as time saved in tuning, troubleshooting, and investigation, reduced risk of security incidents in a regulated environment, and improved operational efficiency by consolidating security and load balancing.."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

Read full review

©2026 PeerSpot, All Rights Reserved

Use Case

"The AOF solution is used for any customer with applications to protect them. It provides security features to protect the application from threats such as SQL injections and challenges of the browser using AI.."

Amr Shawky
Security & Infra Technology Specialist at BARQ Systems

Read full review

"I use F5 Advanced WAF to manage enterprise clients, focusing on licensing and support flexibility to accommodate various customer segments, including enterprises and mid-market customers.."

Validated user
Global Channel Alliances Lead at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"My main use case for F5 Advanced WAF is providing deployment solutions for financial institutions and onboarding their applications on the solution itself. I perform fine-tunings on their solution based on the type of application services that they are hosting on the WAF and also based on traffic behaviors. I provide them with appropriate solutions and tuning requirements for the solution itself.

I deployed F5 Advanced WAF in one of the top-tier commercial banks of Nepal, and I have deployed it in more than two or three banks here. The deployment went from a proof-of-concept state to the deployment stage. Initially, I deployed the proof-of-concept product and tested it on some of their proof-of-concept applications. After that, I deployed it for the production applications. I gradually kept it under tuning and overall monitoring, and after learning the traffic behavior, I moved it to enforcement mode while turning on the blocking part. Initially it started with a monitoring phase and eventually turned into the blocking phase where it starts to protect applications against real attacks.."

Kkc Casey
Security Solutions Architect at a consultancy with 1-10 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"F5 Advanced Web Application Firewall (AWAF) is primarily used in financial sectors like banking to secure web applications against advanced threats, ensuring compliance with industry regulations. Our Key use cases include:

1. **Protection Against OWASP Top 10**: Safeguarding banking applications from SQL injection, XSS, and other common vulnerabilities.
2. **Bot Mitigation**: Detecting and blocking malicious bots to prevent account takeovers, credential stuffing, and fraud.
3. **DDoS Protection**: Defending against application-layer DDoS attacks to ensure service availability.
4. **PCI DSS Compliance**: Enforcing security policies to meet compliance standards for protecting sensitive customer data.
5. **API Security**: Securing APIs used in banking platforms from abuse and unauthorized access.
6. **Threat Intelligence**: Leveraging threat intelligence to identify and mitigate zero-day attacks.
7. **Application Traffic Control**: Managing and monitoring application traffic to ensure optimal performance and security.

These use cases help financial institutions maintain secure and resilient applications, critical for trust and compliance.."

Abdul Azim
Network Security Engineer at a tech vendor with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"My main use case for F5 Advanced WAF is to protect applications and support application delivery, and sometimes we use LTM for load balancing.

A specific scenario where I used F5 Advanced WAF for application delivery was in our banking environment called IDFC First Bank, where we had a critical internet-facing web application used by internet teams and partners that handled sensitive data, and both security and performance were equally important. The application was exposed to the internet and started receiving SQL injections and cross-site attempts, along with automated bot traffic hitting login and search pages. Simultaneously, the traffic load increased, causing slow response times during peak hours, resulting in uneven traffic distribution to the backend servers. We configured the virtual server and pool on F5, enabled health monitors to ensure traffic was sent only to healthy backend servers, and used a load balancing algorithm to distribute traffic. The result was improved application availability, faster response times, and no single backend server overload.

This scenario stands out because it clearly shows how F5 LTM and WAF work together, with LTM focusing on availability and performance, while WAF focuses on security and threat protections, delivering a secure application delivery. The final outcome was that LTM ensures smooth and optimized traffic flow, and F5 Advanced WAF ensures strong application security, keeping the application stable, fast, and secure even during high traffic. It worked reliably in production with 2,000 or more users.."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

Read full review

©2026 PeerSpot, All Rights Reserved

"My main use case for F5 Advanced WAF is to protect external and internal applications from cyber attacks and to prevent malicious payloads and malicious data from reaching servers. Even if malicious content is compromised on the client side and could be executed on the server side before reaching the server, F5 Advanced WAF intercepts the communication and verifies the actual payload and data that the client wants to access or send to the server so that it gets executed securely at the server level.

"I can provide a specific example of how I have used F5 Advanced WAF to protect an application. There was an application where some of the contents actually get loaded from a third-party domain. In that case, the client has to load scripts, images, or any other sort of resources from that third-party domain. When the request reached F5 Advanced WAF, the application sets response headers so that in those response headers, the browser sends the request with the information mentioned in those response headers. Those response headers include Content Security Policy and CORS headers. The domains mentioned there, along with the resources like scripts and images, determine which resources can be accessed. Only those resources are loaded from those domains. If an attacker tries to send the request to a different domain, the browser will not load that. If the application is unable to implement those headers, F5 Advanced WAF can implement or configure those headers so that the resources from the third party get executed or loaded in a secure way. Moreover, if a request comes from the client side, the actual payload is verified because it would be encrypted. This is because whenever we host an application, it should be HTTPS, which means secure communication with F5 Advanced WAF and the server. The client communicates securely. F5 Advanced WAF intercepts everything initiated from the client side, decrypts it with the help of SSL handshake, and there are private and public keys that help encrypt and decrypt the data. F5 Advanced WAF acts as a proxy for that particular application. When a client initiates the request, it seems to the client that they are communicating with the real server, but the request reaches F5 Advanced WAF first instead of the server. F5 Advanced WAF communicates with the client and forwards the data to F5 Advanced WAF. F5 Advanced WAF decrypts the data through SSL handshake. F5 Advanced WAF then verifies what exactly the actual payload contains, whether it is malicious data or legitimate data. F5 Advanced WAF

©2026 PeerSpot, All Rights Reserved

verifies by having predefined attack patterns that contain some attack information. If those attack patterns or malicious data are executed on the server side, that data can compromise server confidentiality and sensitive data. In that case, the actual payload from the client is verified against those patterns. If the data matches those patterns, F5 Advanced WAF enforces the security. If security is in blocking mode, it will stop the request and the blocking reference ID will be forwarded to the client. The client will retain that reference ID. If it is a non-legitimate client, they will be blocked. If legitimate, the client receives the reference ID. Upon receiving the reference ID, the client has to forward it to the company that they are receiving the reference ID while accessing the application, seeking clarification about the issue. The reference ID is verified in F5 Advanced WAF logs, providing insights into what exactly the client sent and what observations were made based on attack patterns triggered by the data. If the client is legitimate, it is treated as a false positive. We then either request the applications team to refactor the way requests are sent or, if cumbersome, relax the policy for that user or URL. This is a granular way to protect against malicious and mitigate false positives for applications deployed on F5 Advanced WAF.

"F5 Advanced WAF has an added advantage over Cloudflare, Barracuda WAF, Imperva WAF, and other WAFs currently in the market. The essential feature is called iRules. With iRules, we can apply two security policies for a single application while segregating user traffic from admin traffic. It is necessary to secure and segregate admin and user traffic because we can implement robust security for user traffic. For admin policy, we can relax the policy since it is an admin resource performing admin functionalities like upgrading the application, integrating resources, or implementing new features. We can simply relax the admin policy and enhance the user policy. One of the most important advantages of F5 Advanced WAF is that we can apply it on the same virtual server where we configure the applications. Other vendors in the market, especially Barracuda WAF, lack such functionality or advanced features. This is a significant advantage that F5 has, and their STM, which handles traffic, is secure and stable.."

Validated user

Senior Security Systems Engineer at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

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.

"The initial setup experience is straightforward, and I did not face any complexities. I recommend deploying the F5 AWAF solution on a single appliance with LTM.."

Abdul Azim

Network Security Engineer at a tech vendor with 11-50 employees

Read full review

"The initial setup of F5 Advanced WAF is straightforward and easy to understand. Without prior training, I could build and publish applications using just the documentation.."

Ahmed Moamen

Senior Security Solutions Architect at Orange

Read full review

©2026 PeerSpot, All Rights Reserved

"Deploying the solution, including initial configuration, licensing, addressing, and enabling WAF, could take one to three hours. However, for a comprehensive setup, considering external factors and optimizations, the process could take up to a month.."

Validated user

Read full review

Senior Network Engineer at a comms service provider with 11-50 employees

"The initial setup involves sending a request, understanding requirements such as policy and application number, and ensuring prerequisites are ready. It uses policy virtual servers and the network WAF, taking about five or six days to implement.."

Amr Shawky

Read full review

Security & Infra Technology Specialist at BARQ Systems

"Deploying the solution involves an application learning and blocking phase. The process includes collecting application data, creating policies, and applying them to lower testing environments like QA or dev before moving to UAT and production. The learning phase is used to handle false positives and fine-tune the policies before going live.."

Habib A

Read full review

Systems Engineer at Sify Technologies

©2026 PeerSpot, All Rights Reserved

"The initial setup of the F5 Advanced WAF solution involves multiple stages and might require revisiting configurations based on customer needs. The setup can be complex compared to other options.."

Ehab Kamal

Import Comliance Specialist at silicon21

Read full review

©2026 PeerSpot, All Rights Reserved

Customer Service and Support

"The customer support for F5 Advanced WAF is fine in itself, though a bit late, but on priority they come in time, so it is not that bad. It is good enough.."

Kkc Casey
Security Solutions Architect at a consultancy with 1-10 employees

Read full review

"The support from F5 is excellent, with resources readily available online. The quality of support depends on the service SLA purchased, with various levels of service provided.."

Ahmed Moamen
Senior Security Solutions Architect at Orange

Read full review

"I find their customer support has experienced and knowledgeable personnel, but their response time could be improved. While they resolve issues well, the time taken for responses to non-critical issues should be shorter.."

Validated user
Senior Security Systems Engineer at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Customer service is very responsive. If the issue persists beyond my local support capabilities, I open a ticket with F5, and they respond quickly. I rate their technical support 9 out of 10.."

Abdul Azim
Network Security Engineer at a tech vendor with 11-50 employees

Read full review

"F5 provides one of the best technical supports, though there have been a few cases where customers were dissatisfied due to response speed. However, in general, their support is highly efficient and knowledgeable.."

Validated user
Senior Network Engineer at a comms service provider with 11-50 employees

Read full review

"My experience with the technical support from F5 is that on the technical side, we sometimes face issues with reachability and availability. Regarding technical support overall, I am not completely satisfied with F5. We are facing problems. I would rate the technical support at five out of ten.

"Both response time and availability need to be improved. Technical skill on the support side also needs improvement.."

Pawan Thakur
Security Analyst at IBM

Read full review

©2026 PeerSpot, All Rights Reserved

Other Advice

"I would fully recommend F5 Advanced WAF for its feature-rich offerings and high detection rate of threats. I rate it a ten out of ten as it is one of the best solutions available.."

Validated user
Senior Network Engineer at a comms service provider with 11-50 employees

Read full review

"I rate F5 eight to nine out of ten. I recommend F5 to customers who require a robust solution and have the budget for it. However, for customers looking for modest pricing, I would not recommend the F5 solution.

I'd rate the solution eight out of ten.."

Abdul Azim
Network Security Engineer at a tech vendor with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"I rate F5 Advanced WAF eight out of ten.

Despite a few issues, F5 Advanced WAF is performing well for me. Improving engagement and enablement for partners would enhance its value to GSI partners and service providers.

Overall, I see potential positive development for the product.."

Validated user
Global Channel Alliances Lead at a tech vendor with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

"If someone is looking into using F5 Advanced WAF, my advice is to spend time on learning and tuning, and do not rely on blocking mode on day one; it is essential to run the application in learning mode, understand traffic patterns, and tune policies properly to avoid false positives in production. Also, it depends on size and platform; while F5 Advanced WAF scales well, correct sizing of hardware and licensing based on traffic volume is crucial. Proper capacity planning upfront saves performance issues later, and having skilled resources is important; this is an enterprise-grade solution, not plug-and-play, so ensure you have experienced F5 engineers or proper training during initial deployment and tuning. F5 Advanced WAF is an excellent choice for large enterprises and regulated environments, but success depends on proper design, tuning, and ongoing review; when implemented correctly, it delivers strong security with stable performance.

Overall, F5 Advanced WAF is a strong, dependable enterprise solution that works best when seen as a long-term security platform rather than a quick add-on; once properly designed, sized, and tuned, it runs quietly in the background and effectively does its job without constant attention. It has met our expectations and proven to be a reliable choice for protecting business-critical applications. I have provided an overall review rating of eight out of ten for F5 Advanced WAF.."

Kallamuddin Ansari
Cyber Security Consultant at HR Software Solution

Read full review

"My advice for others considering F5 Advanced WAF is straightforward: if you foresee your business growing and the potential need for new applications, prioritize security. Ensuring that security is not compromised and maintaining application availability is critical. If budget permits, do not hesitate to invest in F5 Advanced WAF, as it will deliver substantial benefits to your infrastructure over time, rather than opting for cheaper alternatives.

"Companies with adequate budgets should not hesitate to invest in F5 Advanced

©2026 PeerSpot, All Rights Reserved

WAF without considering other vendors. If they want on-prem security for critical, sensitive, and confidential data, F5 Advanced WAF should be the go-to option.

"I measured the 99.9% reduction in malicious requests by utilizing the features of F5 Advanced WAF like DDoS protection, bot protection, enforcement mode of the policy, session awareness, enabled IP intelligence, and other defined features. Every URL is explicitly allowed, with parameters used by those URLs explicitly mentioned. Values for those parameters are tightly controlled. Only certain file types are permitted that are integrated with the application. Additionally, specific enforced parameters include the length of URLs and post data, ensuring that if any application changes occur, requests will be blocked unless they match specified criteria. This creates a positive security model, resulting in 99.9% of the requests being legitimate, with no attacks bypassing F5 Advanced WAF.

"I would rate this product nine out of ten.."

Validated user
Senior Security Systems Engineer at a tech services company with 11-50 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"To assess the effectiveness of DDoS mitigation in F5 Advanced WAF, we checked internally using JMeter, on which we wrote a script and tried multiple users at the same time. The DDoS feature blocked all that traffic according to our threshold. We tested this internally.

"The ability to enforce granular policy adjustments has helped my organization with compliance adherence because in the last three to four months, we put our application in blocking mode. We have not configured granular level settings; we have configured at a high level currently. Going forward, we will be planning to add additional security in the WAF.

"I have not used advanced analytics and traffic insights features. I also have not used vulnerability management features, as we have different solutions for that.

"From my perspective, whatever we have used of F5 Advanced WAF, I do not think it needs improvement because I am currently satisfied with the features provided. We just need to work more on the WAF. If there is anything that needs attention, we will definitely let you know.

"Currently, ten to twelve people are using it in my company. I would rate this solution an eight out of ten.."

Pawan Thakur
Security Analyst at IBM

Read full review

©2026 PeerSpot, All Rights Reserved

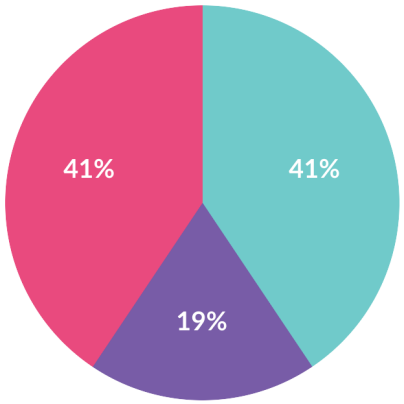
Top Industries

by visitors reading reviews

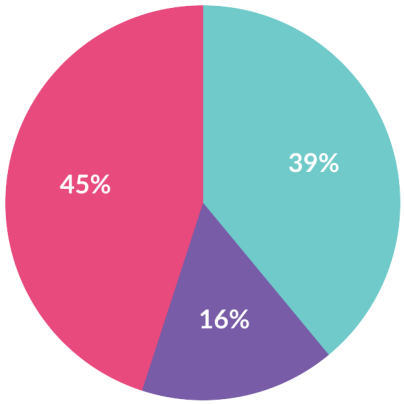
Financial Services Firm	15%
Comms Service Provider	9%
Outsourcing Company	9%
Computer Software Company	9%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved

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

©2026 PeerSpot, All Rights Reserved