aws marketplace

WHITEPAPER

How to Improve Your Security Posture with a Web Application Firewall (WAF)

A SANS Whitepaper

Written by: Serge Borso

Contributor: Geoff Sweet

aws marketplace

Introduction

In the "How to improve your security posture with a web application firewall (WAF)" webinar, SANS and AWS Marketplace shared how a WAF protects web applications by blocking malicious internet-based traffic from reaching them. If you missed the webinar, you can watch it here on-demand.

In this whitepaper, certified SANS instructor Serge Borso discusses how and where a WAF extends the security capabilities of a traditional firewall to stop 90% of the worst types of cyberattacks. You'll also learn the top use cases for a WAF, best practices, and how to use a WAF to meet security compliance requirements.

AWS Marketplace will share how you can integrate a WAF into your AWS cloud.

Partners

The featured solutions for this use case can be accessed in AWS Marketplace:

Fortinet

Barracuda

Cequence

Browse the use cases below and discover popular products that others like you are also using to enhance security in the cloud.

Learn more by visiting AWS Marketplace >

SANS

Analyst Program

Whitepaper

How to Improve Your Security Posture with a Web Application Firewall (WAF)

Written by **Serge Borso**

November 2022

aws marketplace

©2022 SANS™ Institute

Introduction

A web application firewall (WAF) is a security tool used to protect web-facing applications from malicious attacks. Acting as a firewall, a WAF effectively stops malicious content from reaching a web application. Although there are two primary ways to configure a WAF (blocking malicious traffic or simply detecting/learning what malicious traffic is), the most value comes from actively inspecting and thwarting web-based requests that are determined to be malicious in nature. The correct implementation of a WAF is of particular importance because of the prevalence of web applications and the unique attack vectors inherent to a web application. A traditional firewall is a common solution almost every organization will employ; however, a WAF is a purpose-built tool that, despite offering a useful service, is not always deployed for a given workload.

Getting Started with WAFs

In order to effectively block traffic, a WAF is logically deployed between the source of web-based traffic (typically the internet) and the web application being protected (see Figure 1). This is important to note because only in this configuration (or a similar one) can a WAF effectively detect and block malicious traffic destined for the web application. Specifically, the types of attacks a WAF can prevent are centered on the Open Web Application Security Project (OWASP) Top 10 (as well as web application–specific traffic). The OWASP Top 10 is a regularly updated list of the 10 most common and impactful web application vulnerabilities and attacks, which is compiled based on real-world analytics and input from the community.[1] WAF vendors will look to this list to help guide their implementation of a "core rule set" (see Figure 2). A typical WAF will be able to detect and prevent dozens of categories of attacks; the OWASP Top 10 merely serves as a means to categorize the most prominent real-world attacks that are taken into account by WAF vendors.

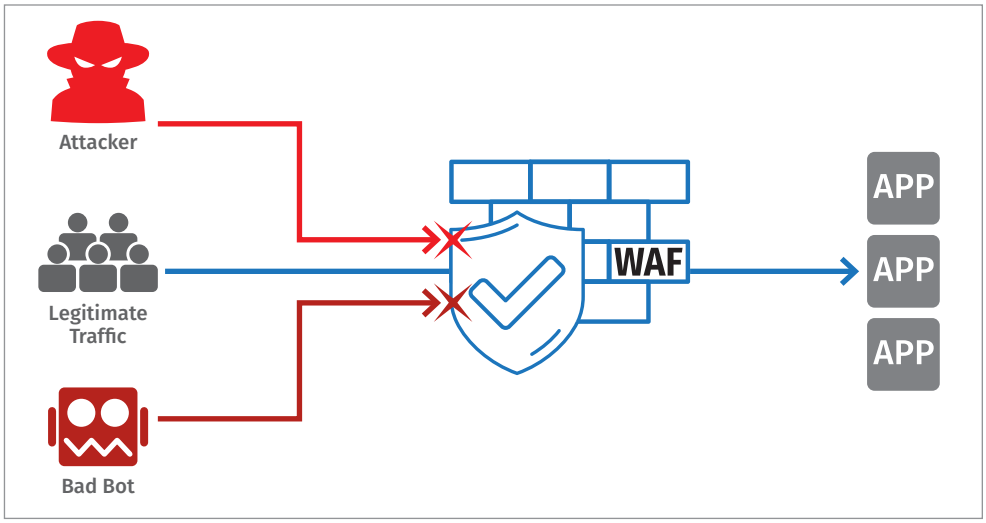


Figure 1. WAF Between a Source and the Application

Figure 2. 2021 OWASP Top 10 List

[1] "OWASP Top Ten," https://owasp.org/www-project-top-ten

A WAF works by leveraging machine in the middle (MITM) functionality, meaning that the device has two specific elements in its configuration: the certificate of the website it is protecting and the associated private key. The SSL/TLS certificate is presented—by the WAF—to the end users/visitors of the website, such that the user agent/browser can confirm validity, whereas the private key is used to decrypt every request being made to the website. Only by performing these functions is the WAF able to inspect the traffic. (Modern-day web traffic is associated with HTTPS websites and therefore is encrypted.) Think of it this way: If a WAF was not able to decrypt traffic, it would have no way to inspect the traffic and ascertain whether the traffic being sent to the application was malicious. A WAF is not a panacea; in reality, even a well-tuned WAF may not be able to stop all categories of attacks, as we explain when we take a closer look at the OWASP Top 10.

A given WAF may excel at blocking injection-based attacks, but add little to no value in the context of identification and authentication failures; it really depends on the use case. There are several logical use cases for WAFs, the main one being centered on enhancing the security posture of a workload by being configured to block malicious traffic, such that the application(s) being protected are less likely to be compromised (using a WAF purely for security reasons). Ideally, if the web application has, for instance, a SQL injection vulnerability, fixing the underlying codebase would be the most appropriate course of action to address the threat. Depending on the software development life cycle (SDLC) and release cycle of the business, however, that injection flaw may not be able to be fixed in a timely manner, if at all (for various reasons—legacy code, third-party product, etc.). In this case, a WAF can add value by protecting the workload, which may not be able to be directly remediated.

Another use case for employing a WAF is to account for enhanced logging—directly addressing Security Logging and Monitoring Failures, number nine on the OWASP Top 10 list. The web applications being protected by the WAF may be working properly, but not employing a type of advanced or security-centric logging, resulting in attacks going unnoticed and useful customer metrics going unmeasured. In this scenario, a WAF would again add value by leveraging its own custom logging capabilities to obtain detailed information about visitors, typical use patterns, and even malicious indicators.

A WAF can be a physical or virtualized appliance deployed on-premises, a cloud-based service tuned to protect a cloud-hosted workload, or even a SaaS-based solution. Depending on the architecture of the network and type of implementation utilized, the configuration of the WAF (as it pertains to the logical placement on the network or within the scope of the infrastructure) will vary significantly. Another aspect of the WAF that will vary significantly is the cost to purchase and operate. A traditional enterprise-class WAF can have a significant upfront cost, which may not include maintenance and support fees. Cloud-based WAF pricing deviates from the flat-fee approach by charging customers per subscription, rule, rule grouping, and the number of requests being inspected (among other potential costs, like bot control, CAPTCHA, geo location blocking, threat monitoring, and other add-on services).

Web applications can be very complex, and the heuristics that are employed by a tool like a WAF can be equally complex. Taking into consideration important information like the language of the application, the types of attacks being submitted, the typical request and response size, character encoding, database technology, API implementation, and other details of the workloads being protected, one can arrive at the conclusion that a WAF is a complex tool in and of itself.

WAFs as a Security Tool

As mentioned, a WAF is not a panacea: Like any other similar security technology, a WAF may have false positives and false negatives. A WAF needs to be tuned and take into account the changes to the workload it is defending. This means that as the core functionality of the workload or protected applications changes, the WAF's configuration also needs to change in order to keep functioning properly. This reality is apparent when new parameters and unexpected payloads or API endpoints are added to the workload—the WAF has to adjust and understand what the "new normal" looks like. Baseline normalcy is of particular relevance in this situation, as the WAF is learning, being tuned, and expected to continue performing optimally without causing issues with legitimate traffic.

These details may result in many businesses being apprehensive (whether they publicly voice this concern or not) about implementing a tool that has the capacity to cause harm to regular business operations—especially a tool that is purposely designed to block web-based traffic. This apprehension can lead to indecision, which manifests in a business choosing to deploy a WAF but configuring the device to be in "learning mode" or "detection mode," where the device merely has the capacity to inspect traffic but not actively prevent attacks. A number of vendors have taken this topic of business apprehension and have specifically designed solutions to reduce the risk of impacting legitimate traffic and help remove apprehension from the conversation.

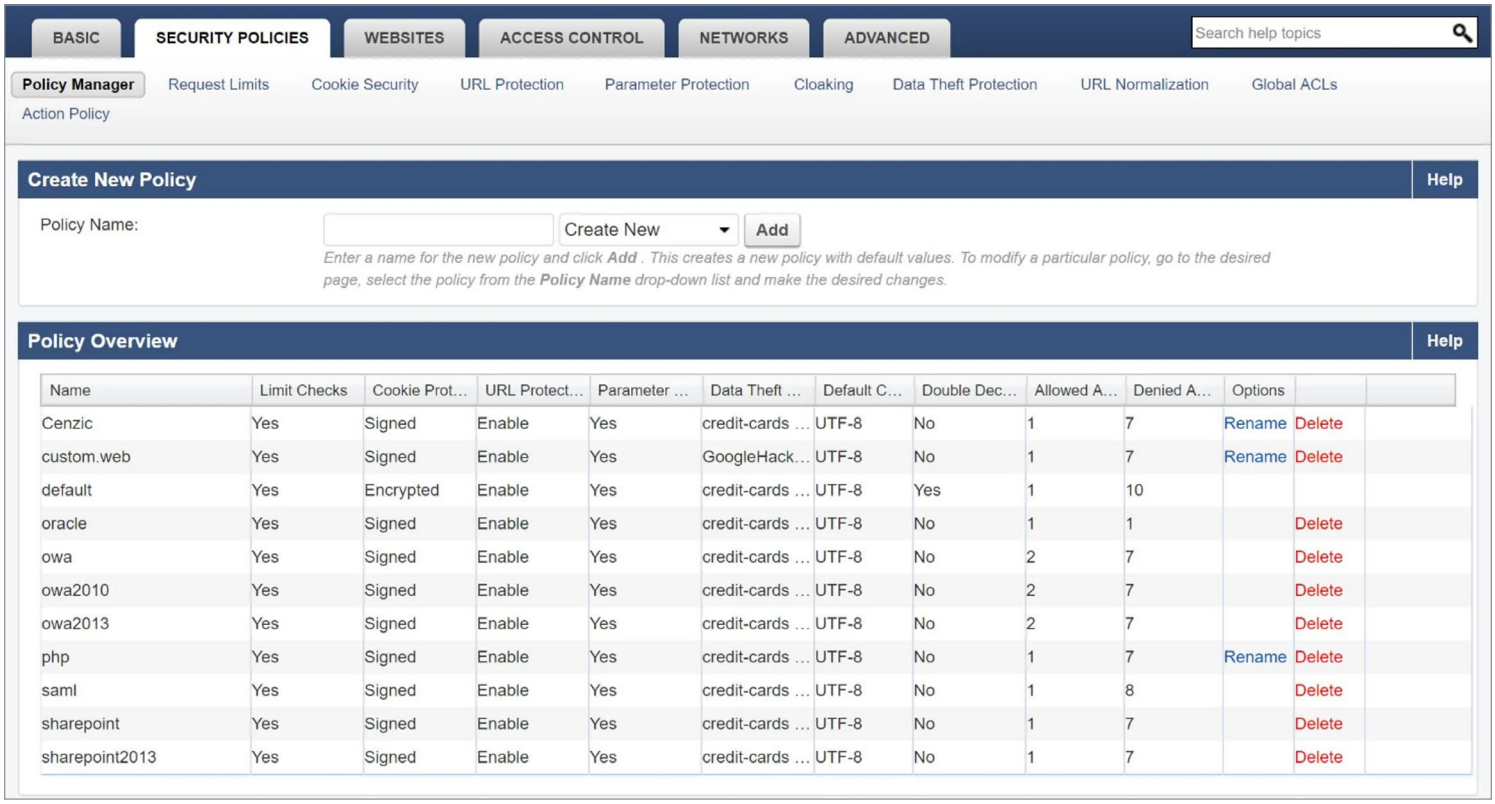
Another interesting reality of WAF services is that WAF functionality often is bundled with other technologies, like load balancing, certificate management, two-factor authentication, and data loss prevention, and a single WAF service/device can be used for multiple purposes. Typically, the networking or security team pitches the idea of implementing a WAF solution. Because of this, using a WAF in an enterprise environment comes with prerequisites, including clear identification of the issues the organization is attempting to solve with the WAF. Note, however, that these concerns have been accounted for by many WAF vendors, because they are not new by any means.

WAF implementations continue to increase, and as they do, it's important for those implementing the technology to maximize the functionality and utilize the full feature set. This is important: A business may purchase the tool but fail to reap the benefits it is paying for (whether the features are used or not). An example of this is API functionality. Modern WAF solutions have a fully featured API that can be integrated with other security tools and services both on-premises and in cloud computing environments. Such an integration would be between an IDS, a WAF, and a network-based firewall. Given this setup, an IDS and a WAF could simultaneously detect suspicious or malicious traffic originating from the same source IP or subnet, and then leverage the API integration between security devices to implement a global network-layer block of the offending IP/subnet for a predetermined period of time. By leveraging the API and performing these actions, a WAF would be able to better serve the entire enterprise by working with other security tools to implement an effective block of malicious traffic at the edge of the network, not just at the application layer.

A modern WAF has many such features as well as extended capabilities that are not typically utilized. Sometimes it takes a bit of imagination to devise useful solutions for a feature; other times, the built-in protections are simply not enabled or set up properly. Examples that fall into this category include bot protections and geographic location blocking. If the entirety of a business's customer population is US-based, then why allow traffic from another country? And therein lies a contributing factor to the lack of feature adoption—lack of expertise in the given technology, lack of confidence in business processes, and lack of buy-in/dedication of time. WAF administrators must take advantage of these features to get the most value out of the tool.

Implementation Best Practices and Compliance

Regardless of where an organization's workload is located (on-premises or in the cloud), the setup for a WAF remains relatively the same—at least at a high level, although the intricacies of each vendor will certainly differ. When deploying a WAF, several components are of concern as they pertain to the proper implementation, location, configuration, tuning, and integration. Location is of relevance, from a logical networking and cloud perspective, because of the importance of placement—the WAF has to be in a position where it can effectively do its job and block malicious traffic. Therefore, it is deployed in line with traffic. This terminology refers to the WAF being positioned between the attacker and the workload being protected, such that malicious traffic from the attacker is directly routed through the WAF for inspection, prior to being filtered/dropped or allowed to flow to the application. Likewise, the configuration of the WAF goes beyond prevention and detection, and speaks to which rules are going to govern the WAF's actions. These rules can be largely built-in rule sets or can be a mixture of custom rules and typical OWASP category matching rules. The rules/configuration are important, however, because they are going to dictate how the tool works—or doesn't work (see Figure 3).



Name	Limit Checks	Cookie Prot…	URL Protect…	Parameter …	Data Theft …	Default C…	Double Dec…	Allowed A…	Denied A…	Options	
Cenzic	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	1	7	Rename	Delete
custom.web	Yes	Signed	Enable	Yes	GoogleHack…	UTF-8	No	1	7	Rename	Delete
default	Yes	Encrypted	Enable	Yes	credit-cards …	UTF-8	Yes	1	10		
oracle	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	1	1		Delete
owa	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	2	7		Delete
owa2010	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	2	7		Delete
owa2013	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	2	7		Delete
php	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	1	7	Rename	Delete
saml	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	1	8		Delete
sharepoint	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	1	7		Delete
sharepoint2013	Yes	Signed	Enable	Yes	credit-cards …	UTF-8	No	1	7		Delete

Figure 3. WAF Rules

WAF rules determine the flow of traffic through the WAF, which either allow or block the traffic, blocking typically being the more common action. Rules work by inspecting the traffic and making a decision about what to do, given the details of the HTTP payload or ancillary information, like source IP address and HTTP headers. For example, if a workload doesn't support the PUT and DELETE HTTP methods, a rule can simply block matching requests. The same concept holds true for traffic that matches a pattern containing a Linux command, a SQL keyword, specific characters in each context, and other patterns of traffic that are deemed potentially malicious.

In addition to security, a WAF can also aid in compliance—and the outcomes can be substantial. For example, under PCI DSS section 6.6, the merchant/processor has two options: Perform a web application penetration test on an annual basis (at a minimum) of all web applications that store, transmit, or process cardholder data, or deploy a WAF. Deploying a WAF is a viable solution and an alternative option to performing penetration testing. However, per the PCI DSS:

> **"Note that compliance is not assured by merely implementing a product with the capabilities described in this paper. Proper positioning, configuration, administration, and monitoring are also key aspects of a compliant solution. Implementing a WAF is one option to meet Requirement 6.6 and does not eliminate the need for a secure software development process (Requirement 6.3)."[2]**

Just having the WAF is not enough for compliance, but proper implementation and maintenance are also required. Many of the other useful features of a WAF can help drive compliance, from data protection to enabling enhanced visibility and monitoring and even gaining insight into data leakage—which can be accomplished by effectively preventing unauthorized data from leaving the application. Because of this, we can look to the WAF to aid with compliance requirements. Another best practice with this in mind is to actually start the deployment process only after identifying application owners. This is relevant because there is not always a single policy (rule set) that will work for all applications. Therefore, in the event there is a negative outcome due to the introduction of a WAF—such as accidentally blocking legitimate traffic—it is important to have the ability to work with business and application owners to address issues in a timely manner.

Another useful feature of a typical WAF is its ability to integrate with the CI/CD pipeline and enhance the security of the SDLC, like other similar security technology. This integration typically revolves around a robust representational state transfer (REST) API and CM tools like Terraform, Chef, Puppet, and the like. Tightly integrating the WAF with the development process not only helps with the advocacy of the WAF, but also reduces the likelihood of unintended results going unnoticed. What will also be of importance is verifying that changes to the WAF flow through the change management process, even for seemingly simple rule changes. This provides transparency and clear communication that something is changing on the security device, which other members of the organization may need to be aware of. Of course, this is not a hard rule; it depends on an organization's implementation, specific vendor, workloads, culture, experience, and intricacies. Approval from a multitude of entities may not be desirable for every rule change.

[2] "Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified," PSI, April 2008, https://listings.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews.pdf

WAFs as a Change Agent

Organizations use WAF technology to enhance the security of a web application or applicable workload, as well as to aid with compliance, adhere to industry best practices, and perform their due diligence. These factors have shifted over time as WAF technology has matured—and with that maturity has come increased adoption of the technology. Cloud computing, too, has lowered the threshold in terms of ease of integration and competitive, albeit potentially convoluted, pricing structures. These realities have culminated in WAFs playing a more prominent role in organizational security, and the results are clear.

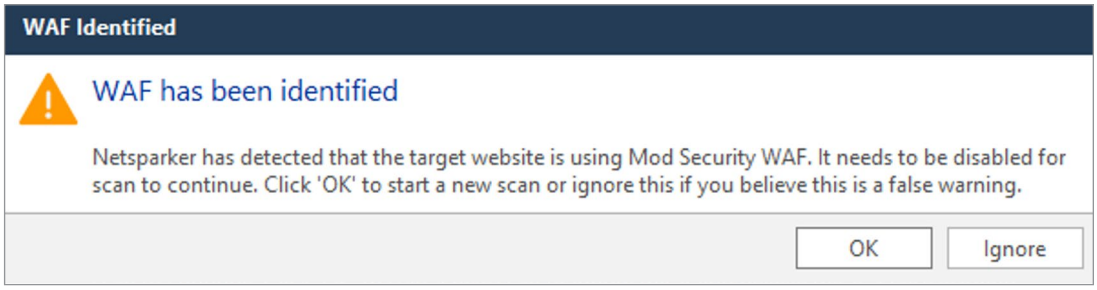


Figure 4. WAF Identified

Having a well-tuned and properly deployed WAF can make a significant difference in an adversary's appetite to target a given web application. Commercial vulnerability scanning tools may cease to even start a robust web application vulnerability scan when they detect the presence of a WAF (see Figure 4).

The benefits of a WAF are real, and the value-added when bundling prevention capabilities with threat-reducing secondary services has resulted in a boon to the security team across organizations. Although there are pitfalls with WAF technology, including blocking legitimate traffic and a need for subject matter expertise, the rewards can outweigh the risks when properly considered. To be clear, although there will always be some risk with any technology, the advancement of modern technology and the maturity of vendor solutions has resulted in a diminishing risk of negative impact, whereas the benefits of implementation can be significant.

A WAF isn't just a piece of technology that protects APIs and websites; WAF technology has matured and grown into a feature-rich solution that organizations rely on for advanced security. This is evident when looking at the machine learning capabilities, DDoS prevention solutions, layer-7 traffic and rule injection features, and even load optimization. Behavioral analysis, for instance, can be leveraged to significantly reduce automated/bot traffic by analyzing traffic patterns based specifically on behavior: What does the request consist of? What is the source of the request (IP/geography/reputation, X-Forwarded-For, referrer, cookie—all spoofable)? Is this known behavior? Is this typical behavior? What is the latency? How likely is it that a human is making the request, as opposed to a bot? WAF technology has progressed and is well situated to take a closer look at traffic coming into the environment and make a security-based decision regarding how best to handle the traffic.

The near-term changes to WAF technology are unlikely to be drastic; they likely will be more subtle over time and in keeping with the significant pace of web technology advancement. Advanced encryption support, tighter API integration with popular services, niche Web 3.0 advancements, more competitive pricing, and select open-source functionality are all likely on the horizon for the WAF technology of the future. In addition, expect to see a continued rise in organization adoption and bundled services, solidifying the "always on" approach, whereby simply deploying a website, some form of WAF technology is enabled by default.

Conclusion

As an application-focused security tool operating at the network layer, a WAF is a unique tool that security-concise organizations utilize to protect their web-based workloads. In an ideally implemented capacity, a WAF will block traffic and increase the security of an organization by effectively shielding web applications and APIs from malicious traffic. This malicious traffic typically falls under a common OWASP Top 10 category, for which rule sets exist to detect and block such threats, effectively rendering the most common attacks benign. Like any advanced security tool, the implementation of a WAF, and adoption of the full feature set, requires a level of expertise and familiarity with business operations, application deployment, and security configurations, which can lead to lack of adoption. This, coupled with convoluted pricing structures and the overarching fear of blocking legitimate traffic when improperly tuned, can lead some organizations to shy away from fully supporting the widespread adoption of the technology.

Nevertheless, a well-tuned and properly implemented WAF helps solve security, compliance, and due diligence use cases for organizations around the globe. By using a WAF, organizations can help control the risk to their organization, protect workloads, enhance logging capabilities, and substantially increase their security posture.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace

aws marketplace

Improve Your Security Posture with a Web Application Firewall (WAF)

Deploy, configure, and integrate a WAF on your AWS cloud

Nearly every organization deploys firewalls, but with the rising use of web applications—as well as their unique attack vectors inherent in them—more effective and targeted security is required. A web application firewall (WAF) sits between a web application and the internet and is purpose-built to fight the most common cyberattacks. Learn how to get started with a WAF and use it as a security tool to protect your web-facing applications.

How AWS customers are leveraging Fortinet to implement a WAF

FortiWeb Cloud WAF-as-a-Service defends web-based applications from known and zero-day threats.
Its AI-based machine learning identifies threats with virtually no false positive detections.
Key features include:

- Advanced threat protection for web applications: Safeguards applications from vulnerability exploits, bots, malware uploads, DDoS attacks, advanced persistent threats (APTs), both unknown and zero-day attacks, and more.
- Low total cost of ownership (TCO): Deployed as a cloud-native SaaS solution in the same AWS Cloud region as an organizations' applications, eliminating the need to maintain hardware or software, and can significantly reduce outbound data transfer costs.
- Simplified compliance requirements: Uses a colony of WAF gateways in the same AWS Cloud region as an organizations' application, potentially avoiding additional regional regulatory requirements.
- Flexible purchasing options: Supports the most suitable option for customers' business priorities and budgetary considerations—whether through pre-provisioned capacity or pay by the volume of processed data.

Why use AWS Marketplace?

AWS Marketplace is a digital software catalog that makes it easy to find, try, buy, deploy, and manage software that runs on AWS. AWS Marketplace has a broad and deep selection of security solutions offered by hundreds of independent software vendors, spanning infrastructure security, logging and monitoring, identity and access control, data protection, and more.

Customers can launch pre-configured solutions in just a few clicks in both Amazon Machine Image (AMI) formats and SaaS subscriptions, with entitlement options such as hourly, monthly, annual, and multi-year contracts.

AWS Marketplace is supported by a global team of solutions architects, product specialists, and other experts to help IT teams connect with the tools and resources needed to streamline migration journeys to AWS.

How to get started with WAF security solutions in AWS Marketplace

Security teams use AWS native services and seller solutions in AWS Marketplace to help build automated, innovative, and secure solutions to address relevant use cases and further harden their cloud security footprint.

Discover WAF solutions in AWS Marketplace >

Explore managed rules for an AWS WAF >

Learn more about Fortinet FortiWeb Cloud >

Connect with an expert >